

HBSS APPLICATION WHITELISTING

TECHNICAL IMPLEMENTATION GUIDE



The Information Assurance Mission at NSA

MIT-001CG-2013

March 2013



Table of Contents

Introduction	3
Background	3
Auditing.....	4
How to create a test group	4
Determine HIPS Version.....	8
Ensure that logging is enabled	12
Create a test policy	16
Importing Policy	23
Applying application whitelisting policies to your test group.....	29
Updating clients with the new policy.....	34
Reviewing Logs.....	37
Querying for Events	37
HIPS 8 workaround	45
Reading query results	46
Tailoring	49
Decision Tree for Execution	50
Visual decision tree	50
Text version of the decision tree	51
Decision tree for modification	53
Visual decision tree	53
Text version of a decision tree	54
Specific Instructions	55
How to Add an Ignore Exception	55
Add a Whitelisted Executable Extension	58
Add a Carefully Constrained Execution Exception	58
Add a Generic Location to the Whitelist.....	60
Check to see if an exception is blocking execution.....	61
Add an exception for an application to execute files with a particular extension.....	62
Add a carefully constrained modification rule.....	64
Enforcement	66
Applying HIPS policies to a group	66
Monitoring	77

Reviewing events	77
How to pick out more important events	77
Remediation and Tailoring when something breaks	78

Introduction

This guide is intended to be used as a reference in implementing location-based application whitelisting using HBSS HIPS. The guide generally lists step by step instructions accompanied by screenshots of each step. By following this guide you should be able to correctly implement application whitelisting using HBSS HIPS.

Background

Things you need to know about your environment before beginning to use this guide:

- Where is the list of approved software?
- Who manages the list of approved software?
- What is the process for Certification and Accreditation (C&A) of software?
- What is the process for obtaining an Approval to Operate (ATO) for software?
- Who is authorized to install and update software on workstations?
- What is the approved process for user to request new software?
- What is the approved process for installing approved software?
- What is the approved process for updating existing software?
- Who has access to the ePO servers?
- Who manages the ePO servers?
- How does one get access to monitor events on an ePO server?
- Who are the POCs in your organization that actively manage the ePO servers' hardware/software?
- Who are the POCS in your organization that manage the HBSS HIPS configurations (rules)?
- ***What is your stance on HBSS HIPS changes and modifications (who approves them, whose responsibility is it to monitor them, what is the process). This is very important. Find out as much information as possible about the process!***

Determine the machines you will use as a test base. These machines will be used to test the initial policy to monitor applications for whitelisting. They will also test the application whitelisting policy as it is being refined by your organization, and they will test the policy when it is modified to block applications on your hosts. Make sure this group is diverse enough to get a good idea of your network variety and setup.

Auditing

Auditing is the first major step that you will take to implement application whitelisting. This will allow you to generate logs that will be useful in creating a policy for your organization. In the auditing phase you will create an application whitelisting test group, create a test policy, import the policy, verify that logging is enabled, apply the policy, and update the test clients with the new test policy.

The auditing step will not block any activity in your environment, it will only monitor and log the events. However, auditing is an essential step for ensuring that approved applications will continue to function properly during enforcement.

How to create a test group

Before you begin you will need to know what machines will be used as a test base. Make sure this group is diverse enough to get a good idea of your network variety and setup. Select either an existing group that will be used for testing or follow the steps below to create new test group. If you are going to use an existing group, you can skip to the next section (Determine HIPS Version).

Log into the ePO server you will be using to create the Group of machines you will use as a test group.

Log On to ePolicy Orchestrator

McAfee | ePolicy Orchestrator 4.5

User name:

Password:

Language:

Copyright 2008-2010 McAfee, Inc. All Rights Reserved.

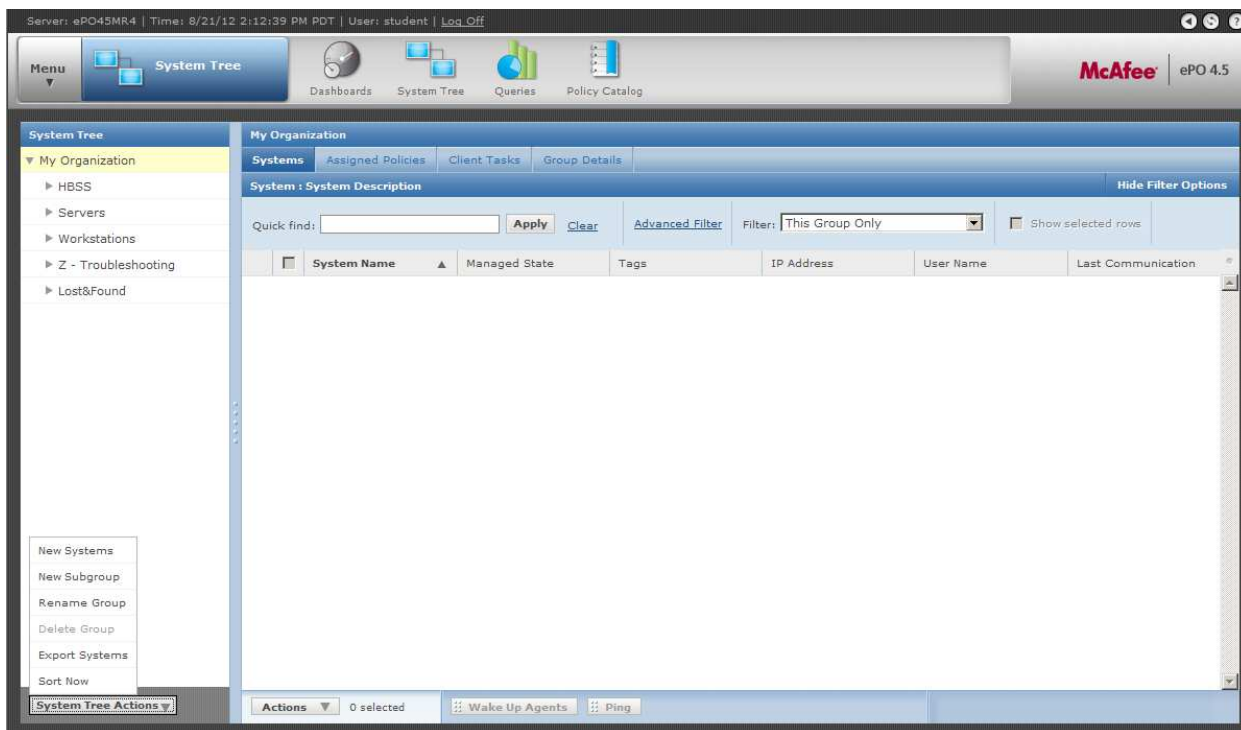
US DEPARTMENT OF DEFENSE WARNING STATEMENT

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

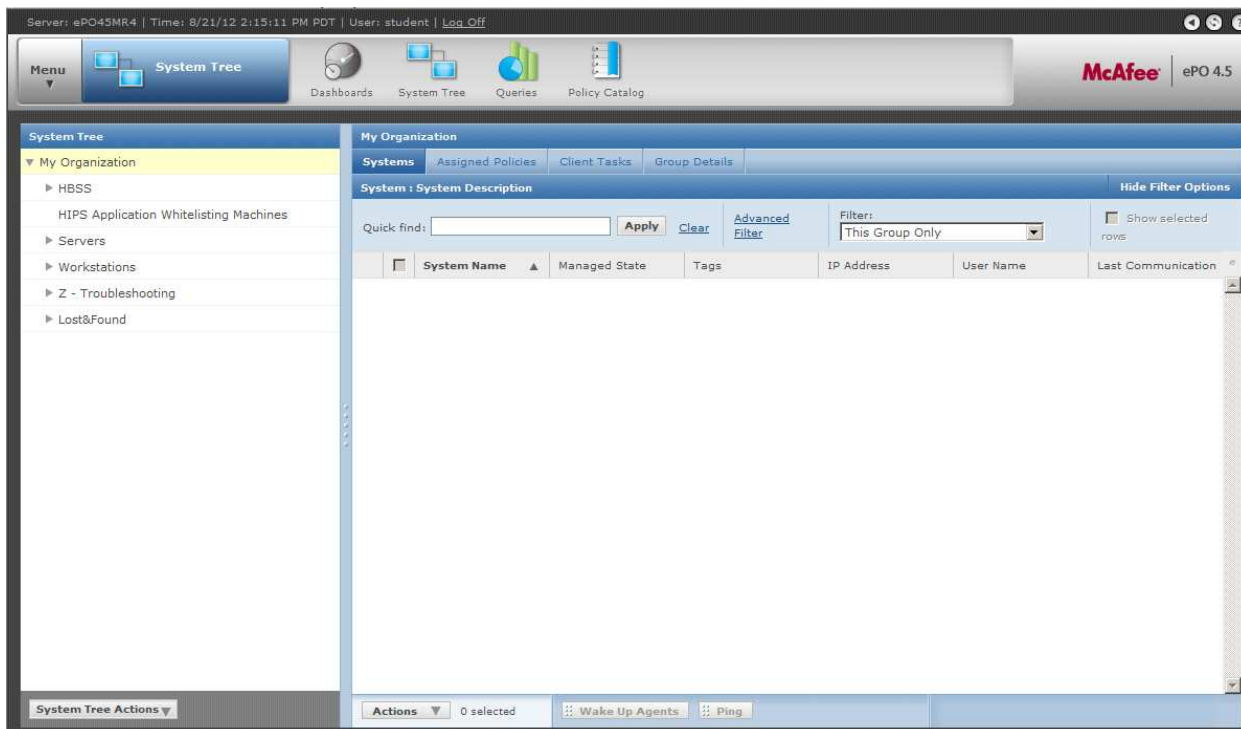
By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

Navigate to the System Tree Tab, Click System Tree Actions, and Click New Subgroup to create a group to add your test machines into. This will create a new container to which you will add your test machines.



Name the new subgroup, “HIPS Application Whiteisting Machines”. You will put all test machines used for HIPS Whitelisting into this container.



Find the systems you want to add to the test group by clicking through System Tree or by searching for the system in the Quick Search - make sure the Filter has “This Group and All Subgroups Selected” if you decide to search for machines using the Quick Search.

Server: ePO45MR4 | Time: 8/21/12 2:15:11 PM PDT | User: student | Log Off

Menu System Tree Dashboards System Tree Queries Policy Catalog McAfee ePO 4.5

System Tree

- My Organization
 - HBSS
 - HIPS Application Whitelisting Machines
 - Servers
 - Domain Controllers
 - Workstations
 - Windows 7
 - Windows XP
 - Z - Troubleshooting
 - Lost&Found

My Organization

Systems Assigned Policies Client Tasks Group Details

System : System Description

Quick find: WIN Apply Clear Advanced Filter Filter: This Group and All Subgroups Show selected rows

	System Name	Managed State	Tags	IP Address	User Name	Last Communication
<input type="checkbox"/>	WIN2K8R2-DC1	Managed	Server	192.168.10.5	student	8/10/12 12:12:10 PM
<input type="checkbox"/>	WIN7CLIENT64	Managed	Workstation	192.168.10.100	student	8/21/12 11:35:46 AM
<input type="checkbox"/>	WIN7CLIENT86	Managed	Install HIPS, Worksta	192.168.10.101	student	8/21/12 12:52:37 PM
<input type="checkbox"/>	WINXPCLIENT86	Managed	Workstation	192.168.10.102	student	8/21/12 1:37:45 PM

System Tree Actions Actions 0 selected Wake Up Agents Ping

Select the systems you want to add to the test group by either dragging or dropping the systems from their old container to the new container you created called “HIPS Application Whitelisting Machines” or select the check box next to the machine name you want to add and click the Action dropdown button, click Directory Management, then click move systems.

Server: ePO45MR4 | Time: 8/21/12 2:15:11 PM PDT | User: student | Log Off

Menu System Tree Dashboards System Tree Queries Policy Catalog McAfee ePO 4.5

System Tree

- My Organization
 - HBSS
 - HIPS Application Whitelisting Machines
 - Servers
 - Domain Controllers
 - Workstations
 - Windows 7
 - Windows XP
 - Z - Troubleshooting
 - Lost&Found

My Organization

Systems Assigned Policies Client Tasks Group Details

System : System Description

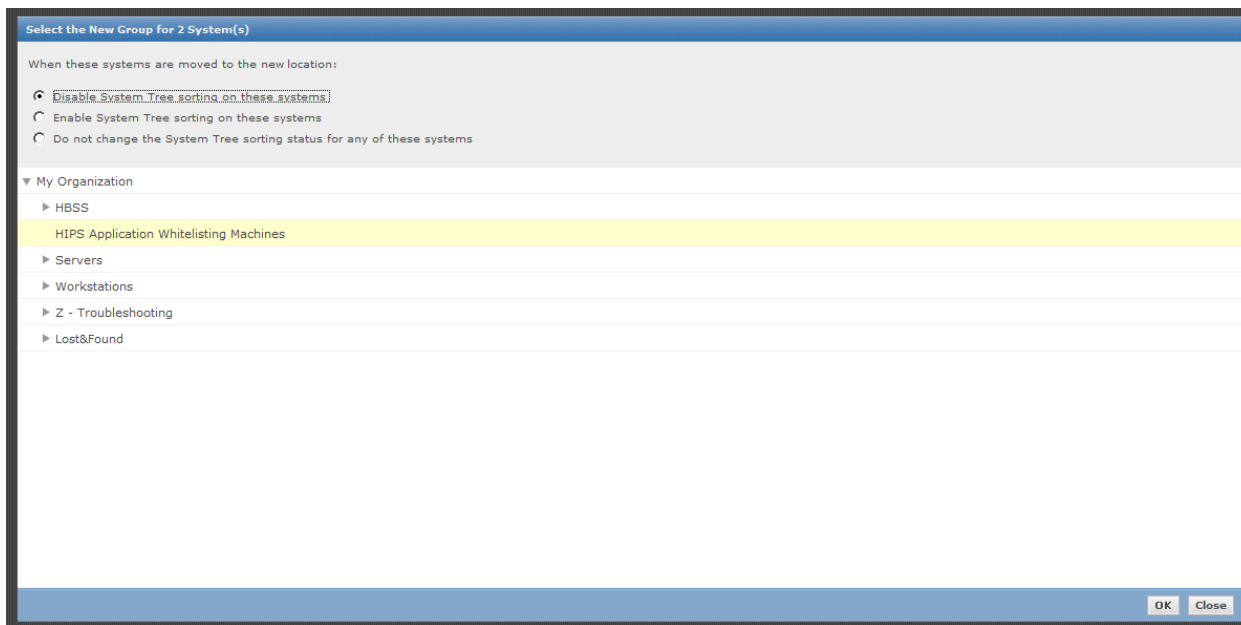
Quick find: WIN Apply Clear Advanced Filter Filter: This Group and All Subgroups Show selected rows

	System Name	Managed State	Tags	IP Address	User Name	Last Communication
<input checked="" type="checkbox"/>	WIN2K8R2-DC1	Managed	Server	192.168.10.5	student	8/10/12 12:12:10 PM
<input checked="" type="checkbox"/>	WIN7CLIENT64	Managed	Workstation	192.168.10.100	student	8/21/12 11:35:46 AM
<input checked="" type="checkbox"/>	WIN7CLIENT86	Managed	Install HIPS, Worksta	192.168.10.101	student	8/21/12 12:52:37 PM
<input type="checkbox"/>	WINXPCLIENT86	Managed	Workstation	192.168.10.102	student	8/21/12 1:37:45 PM

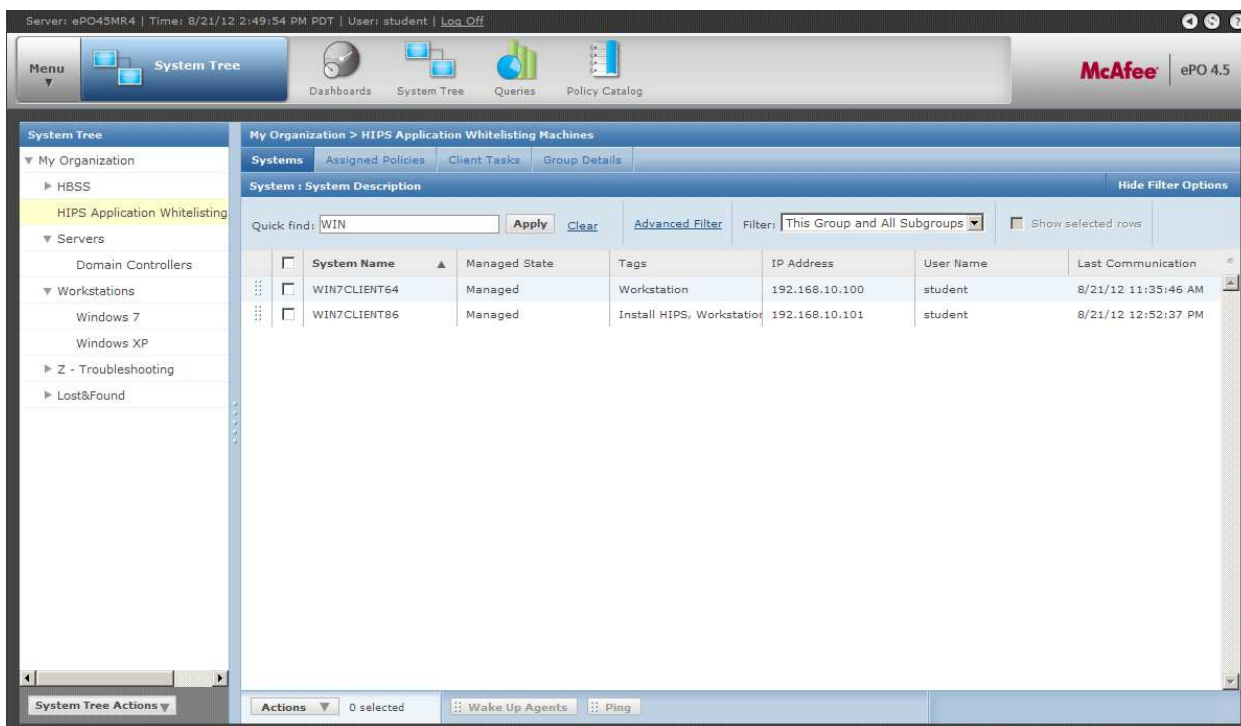
System Tree Actions Actions 2 selected Wake Up Agents Ping

- Change Sorting Status
- Clear Agent GUID Sequence Error Count
- Delete
- Export Systems
- Move GUID to Duplicate List and Delete System
- Move Systems
- Ping
- Sort Now
- Test Sort
- View Effective Policy (by User)

In the next menu prompt, ensure the radio button for disable System Tree Sorting is selected (it should be by default). Next, select the container named “HIPS Application Whitelisting Machines”. Click Ok. These actions will move the machines from their old container to the newly created container.



Double click the Container called “HIPS Application Whitelisting Machines” to check to make sure the systems have been added to the test group correctly. You should see something like this (except with whatever machine names you selected).



Repeat the steps above to add any remaining test machines to the testing container.

Determine HIPS Version

Log into the EPO server.

Log On to ePolicy Orchestrator

McAfee | ePolicy Orchestrator 4.5

User name:

Password:

Language:

Copyright 2008-2010 McAfee, Inc. All Rights Reserved.

US DEPARTMENT OF DEFENSE WARNING STATEMENT

You are accessing A U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

Go to the “Queries” Tab and select “New Query”.

Server: ePO45MR4 | Time: 8/23/12 10:21:37 AM PDT | User: student | [Log Off](#)

Menu **Queries** Dashboards System Tree Queries Policy Catalog

McAfee | ePO 4.5

Groups

- All Queries
- My Groups
- Shared Groups

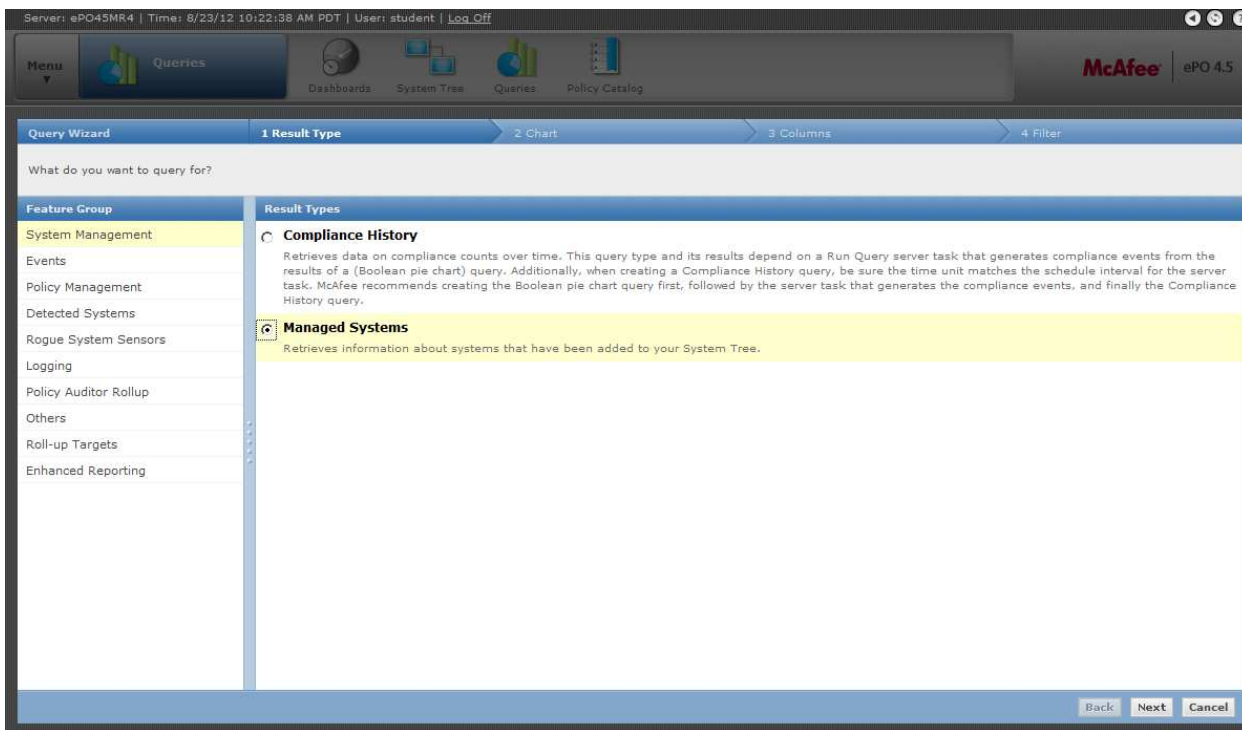
Queries

Quick find: ☐ Show selected rows

☐ Queries Actions

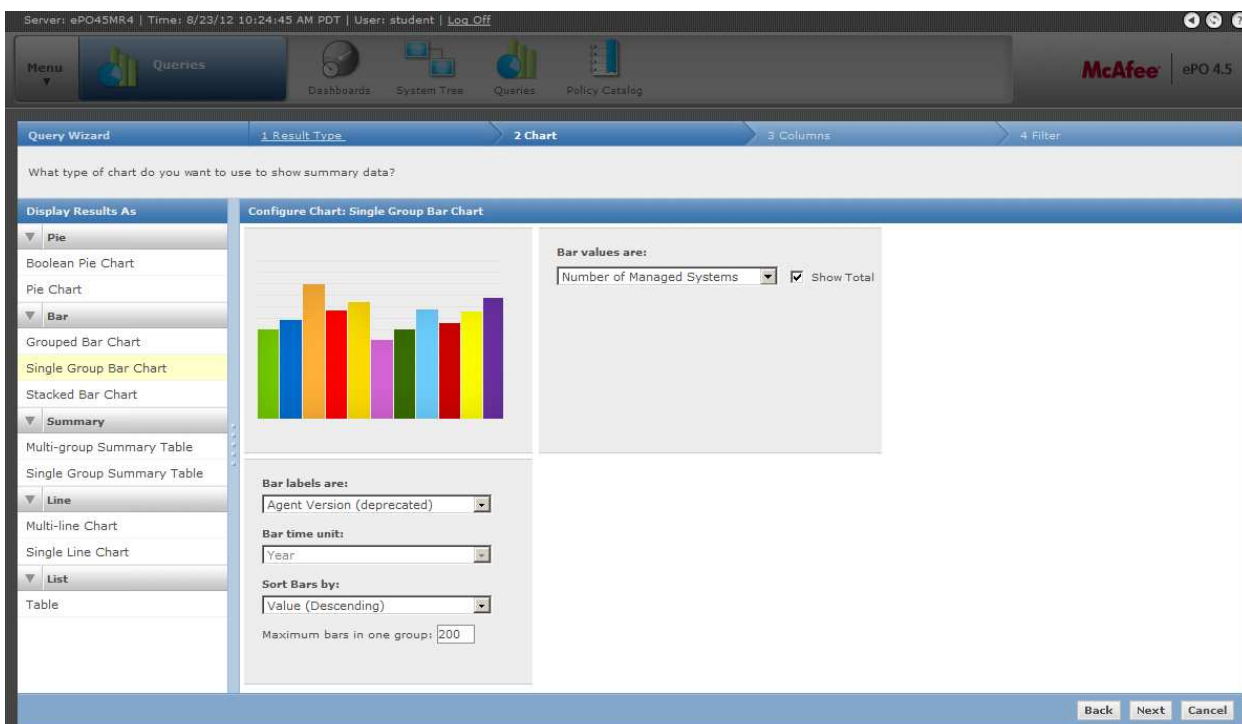
Group Actions Actions 0 selected

A new window will be displayed showing the different types of queries that can be run. Select “System Management” and then select the “Managed Systems” radio button in the “Query Wizard” part “1 Result Type” portion. *If you do not see these options you will need to talk to an administrator to run this query for you.*

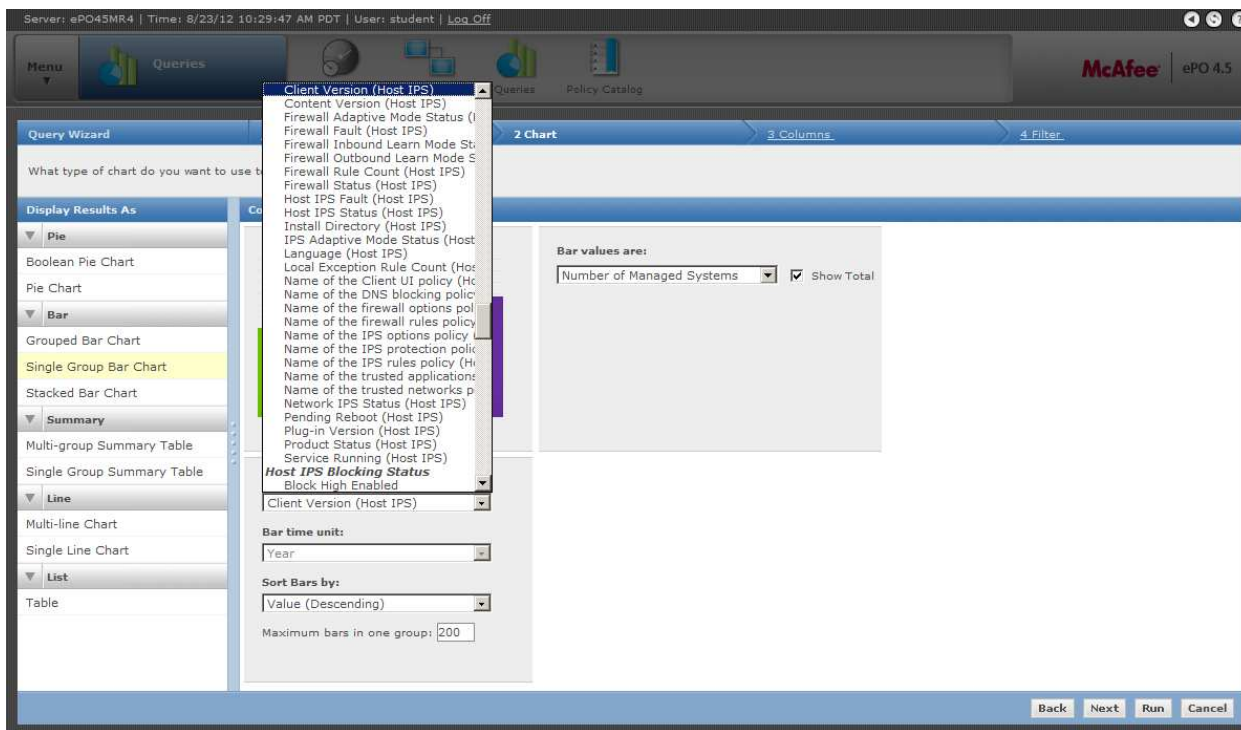


Click “Next” to proceed to the next step.

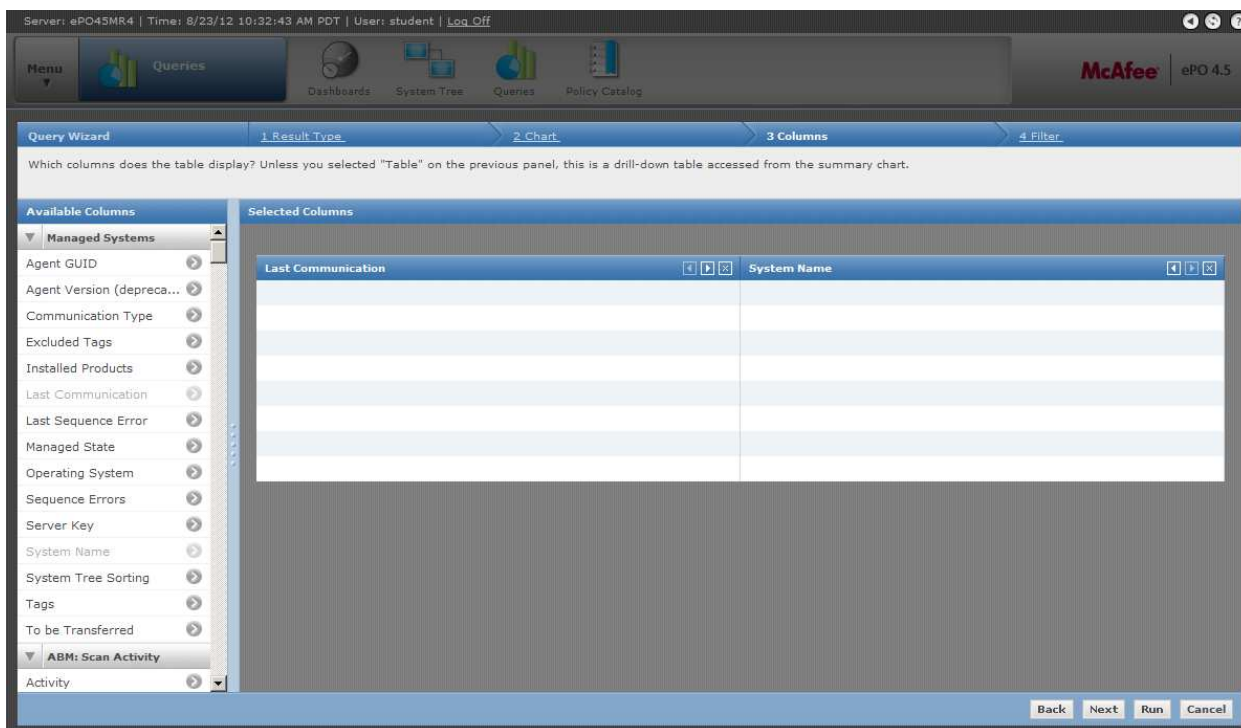
Select the “Single Group Bar Chart” option on the right hand menu under the “2 Chart” Portion of the “Query Wizard”.



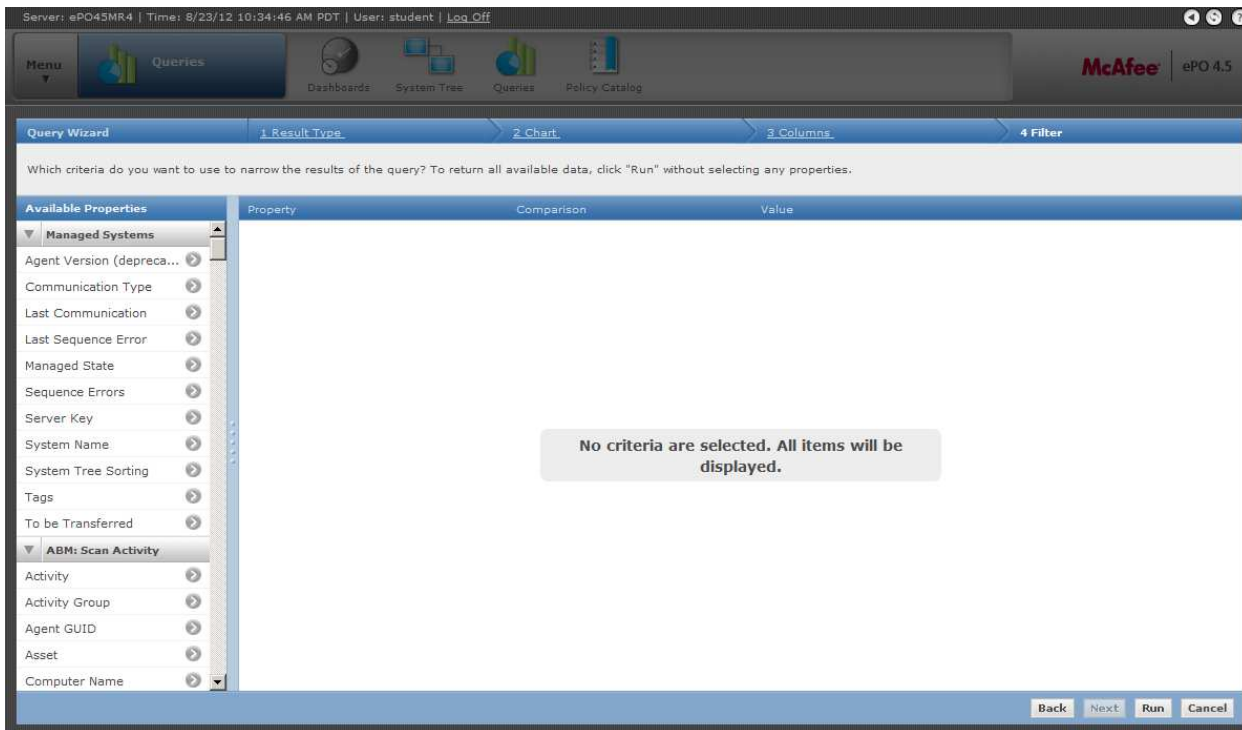
Change the “Bar Labels are” dropdown menu to “Client Version (Host IPS)”. There are many options in the dropdown menu, so make sure you have selected the correct one. After you have selected the correct field, click “Next” to proceed to the next step.



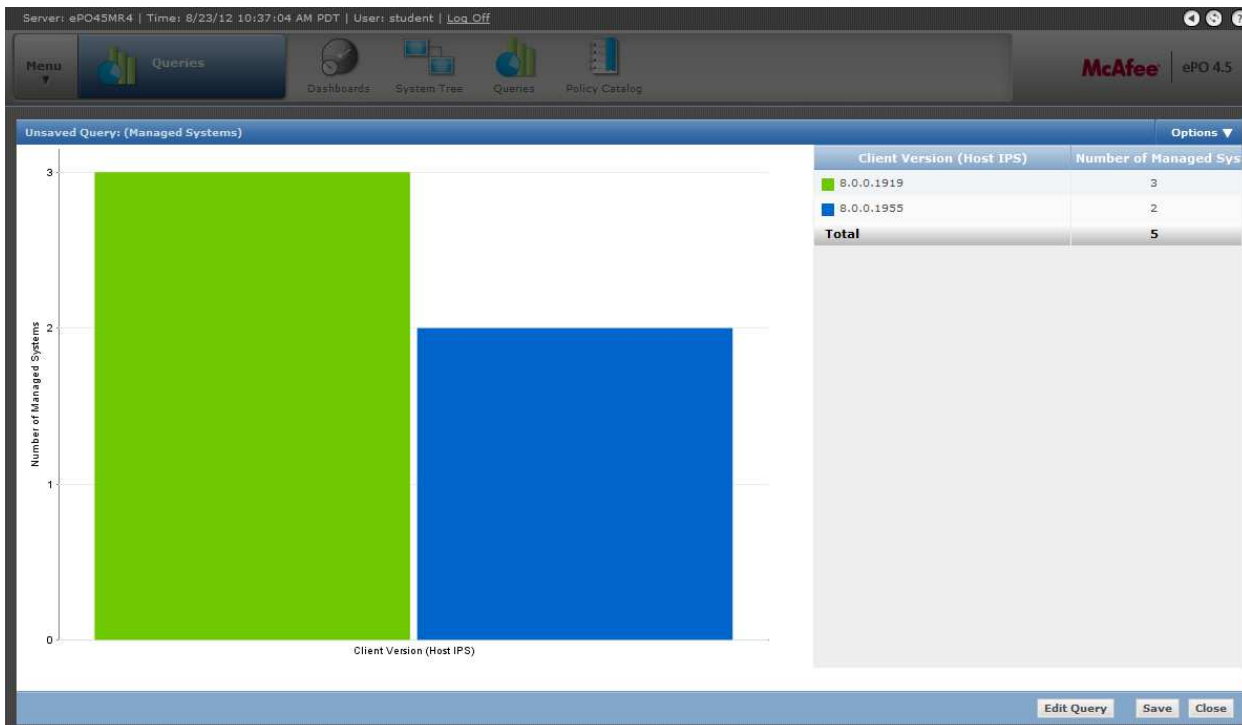
You do not need to modify anything in the “3 Columns” Portion of the “Query Wizard”. Just click “Next” to proceed to the next screen.



You do not need to modify anything in the “4 Filter” Portion of the “Query Wizard”. Click “Run” to see the results of your query.



You will see a graph similar to the one below once the query has completed running. Now let's determine what information the query has shown us.



Your graph will look different depending on which version of HIPS you are running. You will be using the HIPS policy that is applied to the majority of your machines (7 or 8). Only the primary version number is of interest to us. In the case above, you can see that the machines are all running some version of HIPS 8. Congratulations, you have discovered which versions of HIPS are reporting to your ePO server! *Take note of what version is running on the majority of your machines, you will need this information later.*

Ensure that logging is enabled

First, check to see if the existing protection policy has logging enabled for any severity levels. Log in to the ePO server. Navigate within the “System Tree” to your test container. Click on the “Assigned Policies” tab and select either “Host Intrusion Prevention 8.0:IPS” or “Host Intrusion Prevention 7.0.5:IPS” depending on what version you are running. Click on the policy name for the “IPS Protection (All Platforms)”. Check if any of the Severity levels are set to have a Reaction of Log. If so, take note of that severity level because you will set that same severity level in the HBSS Application Whitelisting Configuration Utility. If there are no Severity levels that are currently set to Log in the IPS Protection policy, then follow the instructions below to create a new IPS Protection policy which will set the Information Severity level to a reaction of Log.

Log into the ePO server.

Log On to ePolicy Orchestrator

McAfee | ePolicy Orchestrator 4.5

User name:

Password:

Language:

Copyright 2008-2010 McAfee, Inc. All Rights Reserved.

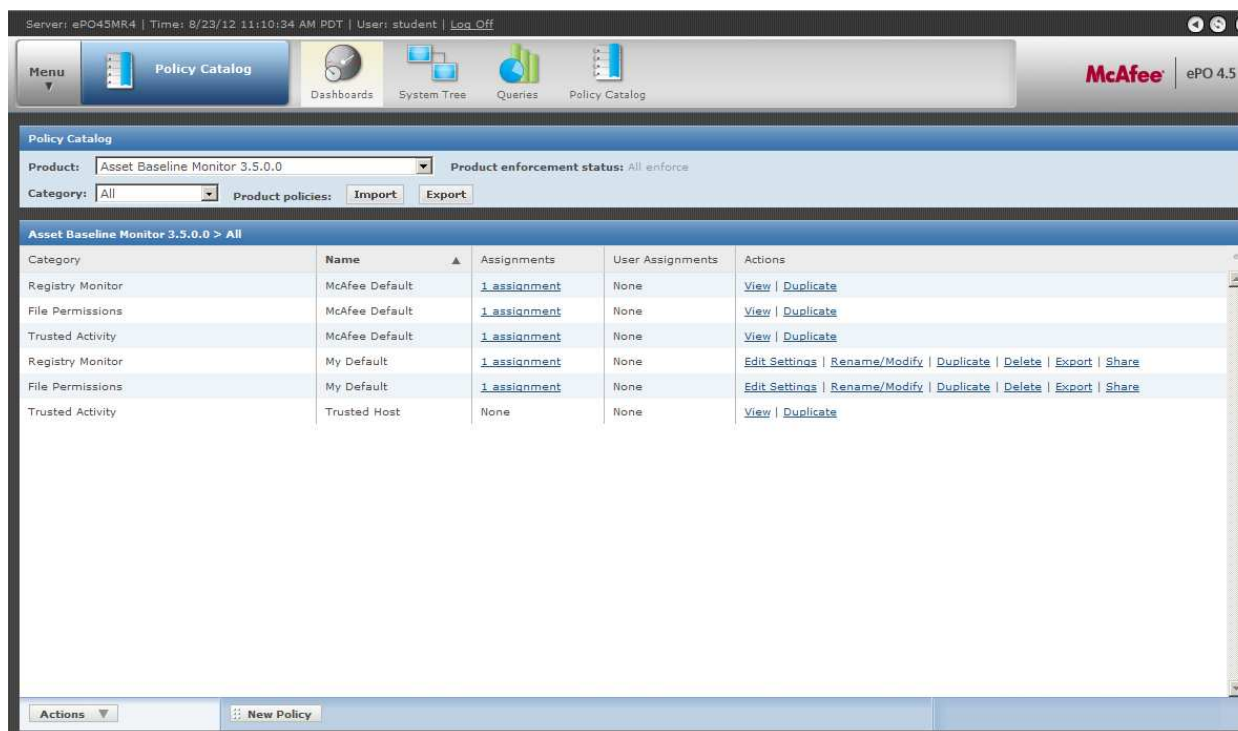
US DEPARTMENT OF DEFENSE WARNING STATEMENT

You are accessing A U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

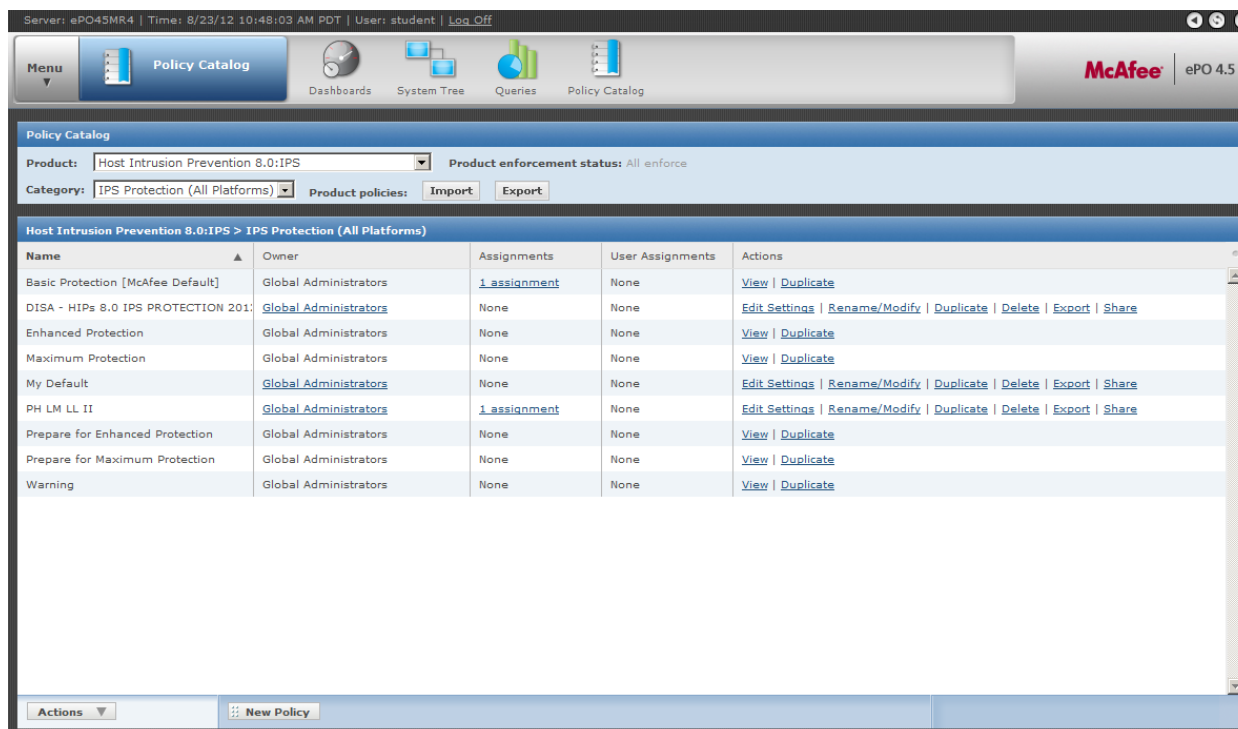
- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

Navigate to the “Policy Catalog” tab.

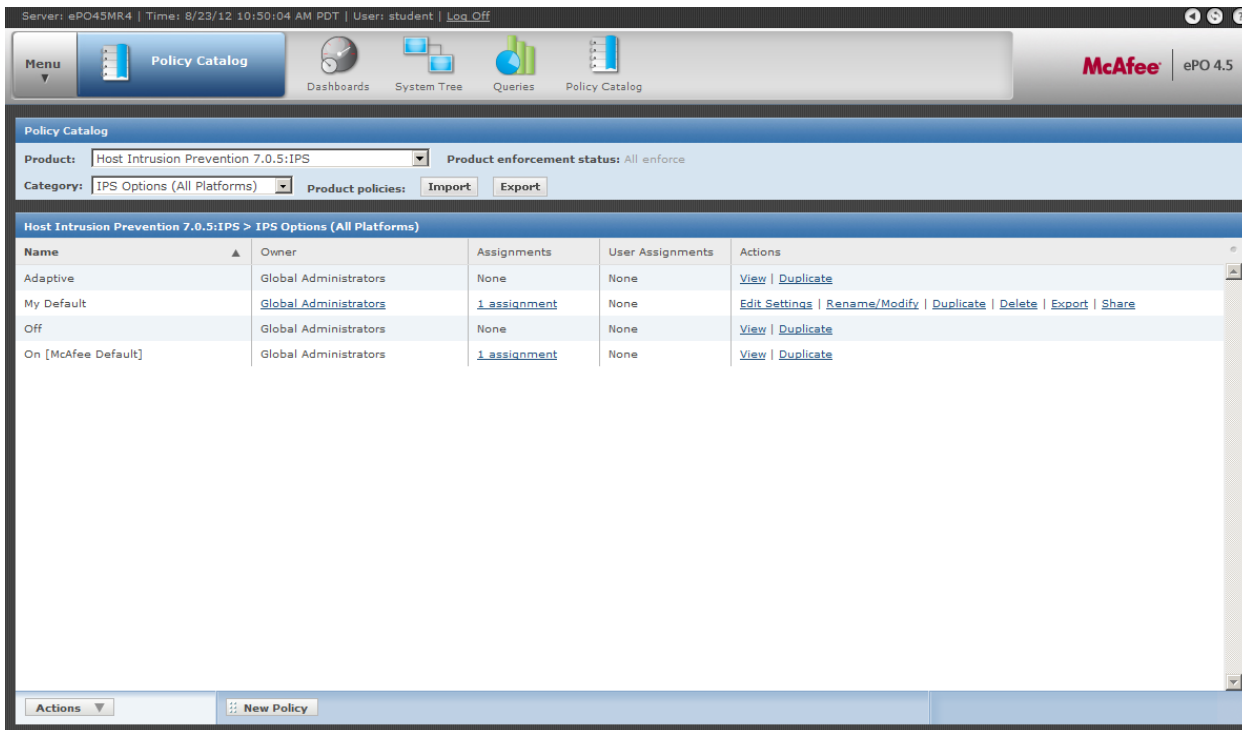


Select the Correct Version of HIPS in the “Product” dropdown menu (in the example below, we are running HIPS 8). The Name you will select will be similar to “Host Intrusion Prevention 7.0.5:IPS” or “Host Intrusion Prevention 8.0:IPS” depending on which version you are running. It will look like one of the following screens depending on your version:

This is if you are running HIPS 8:

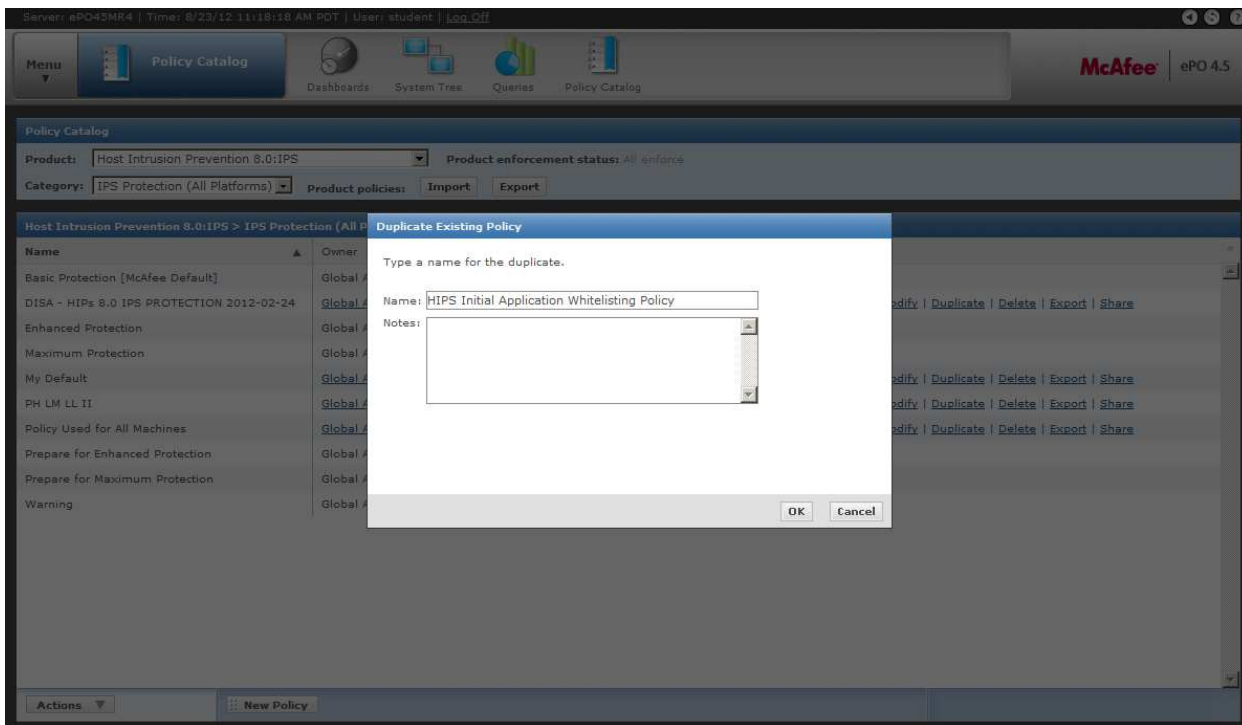


This is if you are running HIPS 7:



Next, regardless of your version, you will select the “IPS Protection (All Platforms)” in the “Category” dropdown menu (which is located below the “Product” dropdown menu).

Find the HIPS Protection Policy being applied to “My Organization”. Click “Duplicate” to create a new HIPS Protection Policy to be used for testing. Name the Protection Policy. It will look as follows:



Click “OK”. You will see your new policy added to the HIPS Protection Policy List as shown: We duplicated a policy called “Policy Used for All Machines” and named the duplicated policy, “HIPS Initial Application Whitelisting Policy”. We can see the policy we duplicated in the list.

Server: ePO45MR4 | Time: 8/23/12 11:24:07 AM PDT | User: student | Log Off

Menu Policy Catalog Dashboards System Tree Queries Policy Catalog

Product: Host Intrusion Prevention 8.0:IPS Product enforcement status: All enforce

Category: IPS Protection (All Platforms) Product policies: Import Export

Host Intrusion Prevention 8.0:IPS > IPS Protection (All Platforms)

Name	Owner	Assignments	User Assignments	Actions
Basic Protection [McAfee Default]	Global Administrators	1 assignment	None	View Duplicate
DISA - HIPs 8.0 IPS PROTECTION 2012-02-24	Global Administrators	None	None	Edit Settings Rename/Modify Duplicate Delete Export Share
Enhanced Protection	Global Administrators	None	None	View Duplicate
HIPS Initial Application Whitelisting Policy	Global Administrators	None	None	Edit Settings Rename/Modify Duplicate Delete Export Share
Maximum Protection	Global Administrators	None	None	View Duplicate
My Default	Global Administrators	None	None	Edit Settings Rename/Modify Duplicate Delete Export Share
PH LM LL II	Global Administrators	1 assignment	None	Edit Settings Rename/Modify Duplicate Delete Export Share
Policy Used for All Machines	Global Administrators	None	None	Edit Settings Rename/Modify Duplicate Delete Export Share
Prepare for Enhanced Protection	Global Administrators	None	None	View Duplicate
Prepare for Maximum Protection	Global Administrators	None	None	View Duplicate
Warning	Global Administrators	None	None	View Duplicate

Actions New Policy

Now click “Edit Settings” for the policy you have just created. A screen similar to the one below will be displayed.

Server: ePO45MR4 | Time: 8/23/12 11:25:05 AM PDT | User: student | Log Off

Menu Policy Catalog Dashboards System Tree Queries Policy Catalog

McAfee ePO 4.5

Host Intrusion Prevention 8.0:IPS > IPS Protection (All Platforms) > HIPS Initial Application Whitelisting Policy

Reaction based on signature severity level:

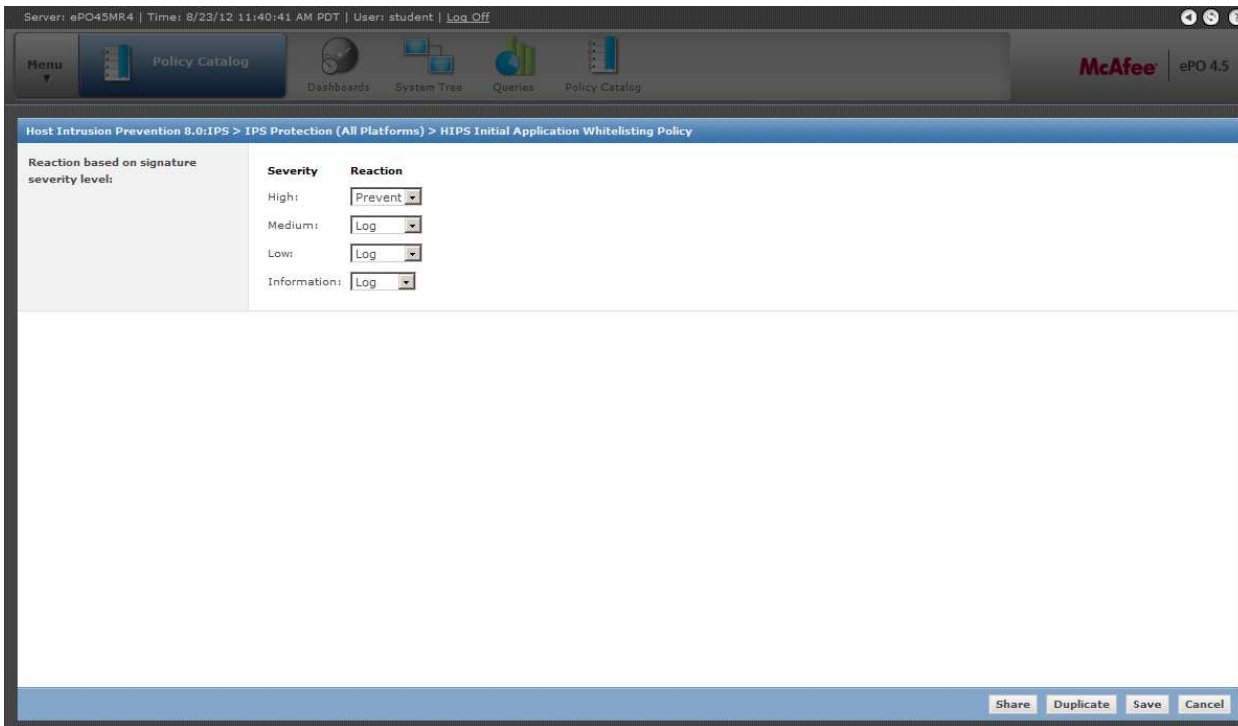
Severity	Reaction
High:	Prevent
Medium:	Ignore
Low:	Log
Information:	Ignore

Share Duplicate Save Cancel

Make sure the “Information” dropdown is set to “Log” to ensure that all Application Whitelisting Signature events will be sent to the ePO server without actually blocking them.

At this step, make sure you follow your organizations policy for reporting informational events to not flood the EPO server with events. Setting informational signatures to "log" could generate a large number of events if you had informational signatures set to "ignore" in the past. If this is the case, make sure you disable all other informational signatures in your HIPS policy.

Your policy will have informational signatures set to “Log” and will look similar to the screenshot below.



Click “Save” to save your Application Whitelisting IPS Protection Policy to the ePO server.

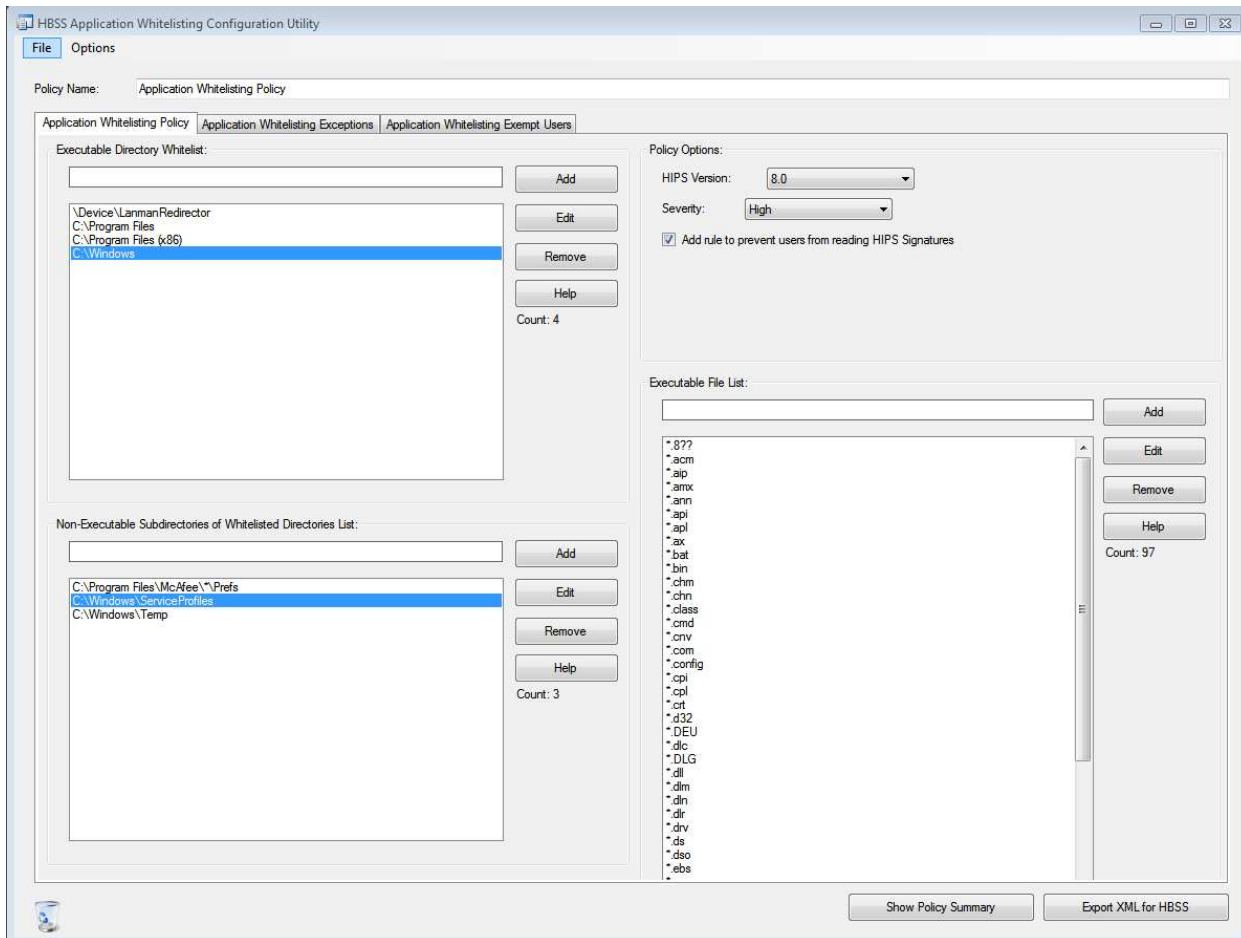
Create a test policy

Obtain and run the HIPS application whitelisting tool.

Remember that your initial test with creating this policy will not block any activity in your environment, it will only monitor and log the events.

NOTE: *The application whitelisting policy can only target one version of HIPS at a time. If HIPS 8 is selected then clients running HIPS 7 will not apply the policy, and vice versa. To target both HIPS versions 7 and 8, two separate policies would need to be used.*

The tool will open to look like the following:

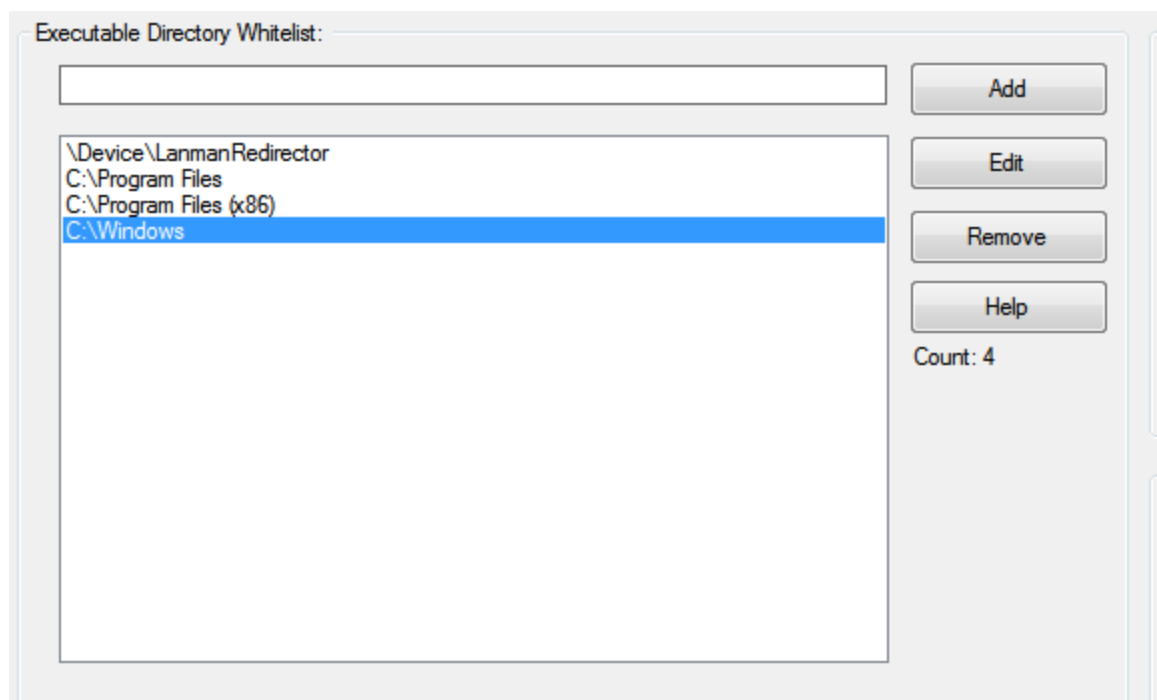


Take the following steps to create a basic baseline policy to conduct your initial test in your environment.

Name the policy. The policy name is listed toward the top of the GUI and by default is called “Application Whitelisting Policy with HIPS 8.0”. (Make sure you use a unique policy name every time you create a new policy to be applied to a different set of computers, since duplicate policy names could cause accidental deletion of the previous policy when importing to the EPO server. However, when updating the policy to be applied to the same computers, reuse the existing name so that importing the policy will update the existing policy on the EPO server and it will immediately be applied to the previously assigned computers.)

Remember that our initial test with creating this policy will not block any activity in your environment, it will only monitor and log the events.

Executable Directory Whitelist contains the locations where program executions are allowed. Organizational policy will dictate what directories will be allowed in your environment. Some basic directories have been included by default.

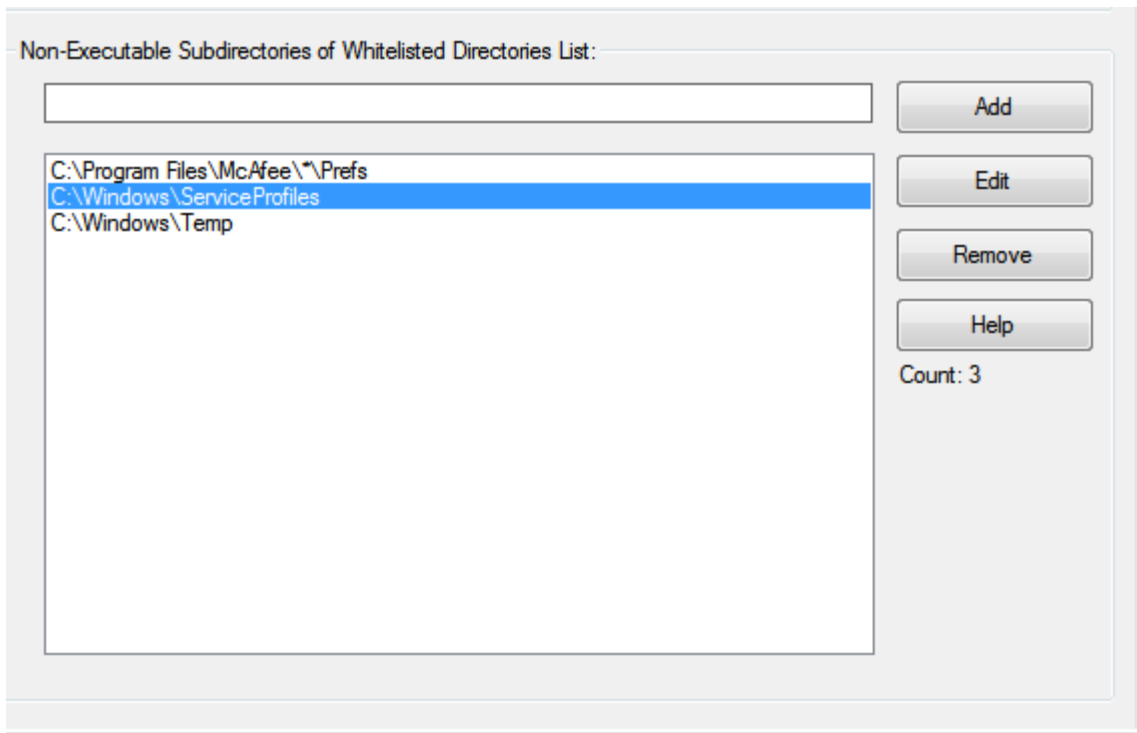


Use the add, edit, and remove keys to modify the list of directories to match your organization's configuration, or use the default configurations as a test. To add a directory, enter the name of the directory in the text box and click the "Add" button. To edit an already existing entry, select the entry, click the edit button, modify the entry as needed, and then click the "Add" button to add the entry back into the list. To remove an already existing entry, select the entry, and click the remove button.

Add standard application installation locations for your network (e.g., "D:\Programs") and file server shares where many users will run applications and scripts from. For example, many domains run user logon scripts as part of Group Policy from the domain controllers' SYSVOL share, so those shares should be added to this list. As can be seen by clicking on the help button, wildcards can be used to reduce the number of entries needed and for added flexibility. For the user logon scripts example, if the domain controllers have a naming scheme of the form USCC-DC-01 through USCC-DC-05, then "\\USCC-DC-??\SYSVOL" should be added to the list to cover all the existing server shares and allow for additional servers in the future.

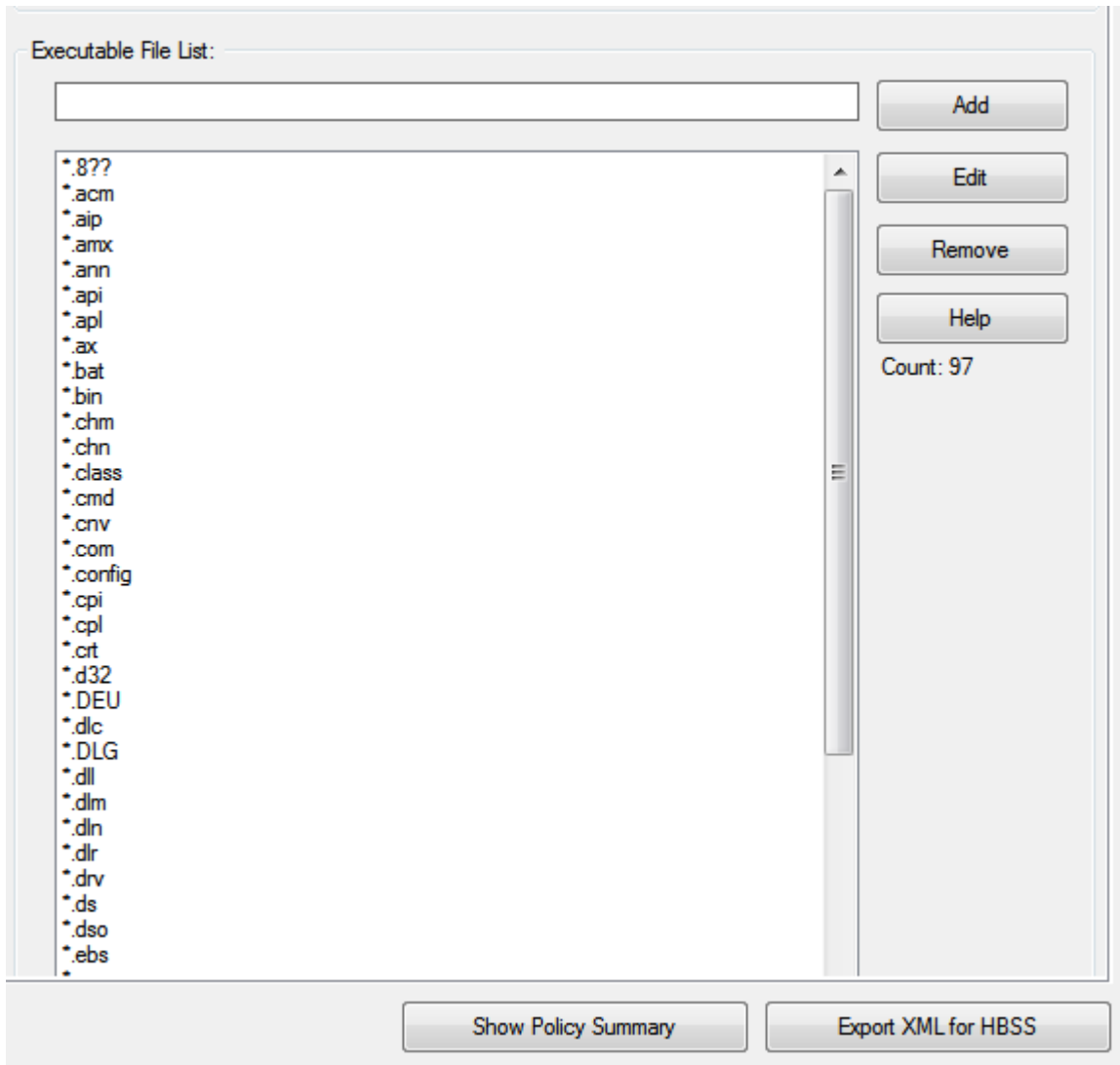
(NOTE: You cannot edit or remove the default entries)

The **Non-Executable Subdirectories of Whitelisted Directories List** are the directories within the whitelisted directories where normal users will need to be able to add or modify executable file types, but not execute them. This means that users can store, read, and write data from these locations, but cannot execute any programs from the directories.



Remember that your initial test with creating this policy will not block any activity in your environment, it will only monitor and log the events.

The **Executable File List** specifies the file extensions for the executable file types that will be allowed to be executed, but not modified, by normal users. You can leave this list the way it is for now.



Remember that your initial test with creating this policy will not block any activity in your environment, it will only monitor and log the events.

The **Policy Options** determine the format of the policy. The HIPS version creates a unique policy for HIPS 7.0 or 8.0. Choose the version currently running on your environment. Select “informational” from the severity dropdown unless logging was selected for another level, if it was, then select that severity level. Make sure the check box for adding a rule to protect the signatures is selected.

Policy Options:

HIPS Version:

Severity:

☒ Add rule to prevent users from reading HIPS Signatures

The **Application Whitelisting Exceptions Tab** details applications that are whitelisted that require constrained exceptions to the application whitelisting policy in order to function properly. Each entry in the exception description section represents an approved application being whitelisted. Clicking on an entry will display the process or processes and the files that the processes are allowed to execute or modify. You can add, edit, and modify the entries just as before. Note that each “Add”, “Remove”, and “Edit” button only affects the entries for a specific list. For this initial test the “Block without logging” option does not result in any actual blocks on the client (everything will be at most logging only). This tab will not be used in your initial test, but will be used to fine tune your policy once event data is obtained from your test group.

HBSS Application Whitelisting Configuration Utility - Application Whitelisting Policy1.policy

File Options

Policy Name: Application Whitelisting Policy

Application Whitelisting Policy Application Whitelisting Exceptions Application Whitelisting Exempt Users

Exception Description:

☐ Allow
☐ Block without logging

Add Edit Remove Help

Count: 18

Description	Type
Exempt Adobe access to common adobe files	Allow
Exempt Adobe Flash Player for IE8 to function	Allow
Exempt Cardscan needs to execute its own dat file	Allow
Exempt Citrix	Allow
Exempt Google Earth Plugin	Allow
Exempt Gradkell DBsign Data Security Suite	Allow
Exempt Juniper	Allow
Exempt Macromedia Flash - used in DCO sessions	Allow
Exempt Microsoft Office programs executing lex files	Allow
Exempt Microsoft programs executing fltr.dat files	Allow
Exempt Print Spooler for printing	Allow
Exempt Reflection Web Plugin	Allow
Exempt Symantec VirusTray	Allow

Exception Processes:

Process:

Add Edit Remove Help

Count: 2

Exception Files Being Accessed:

File: for: ☐ Execution ☐ Modification

Add Edit Remove Help

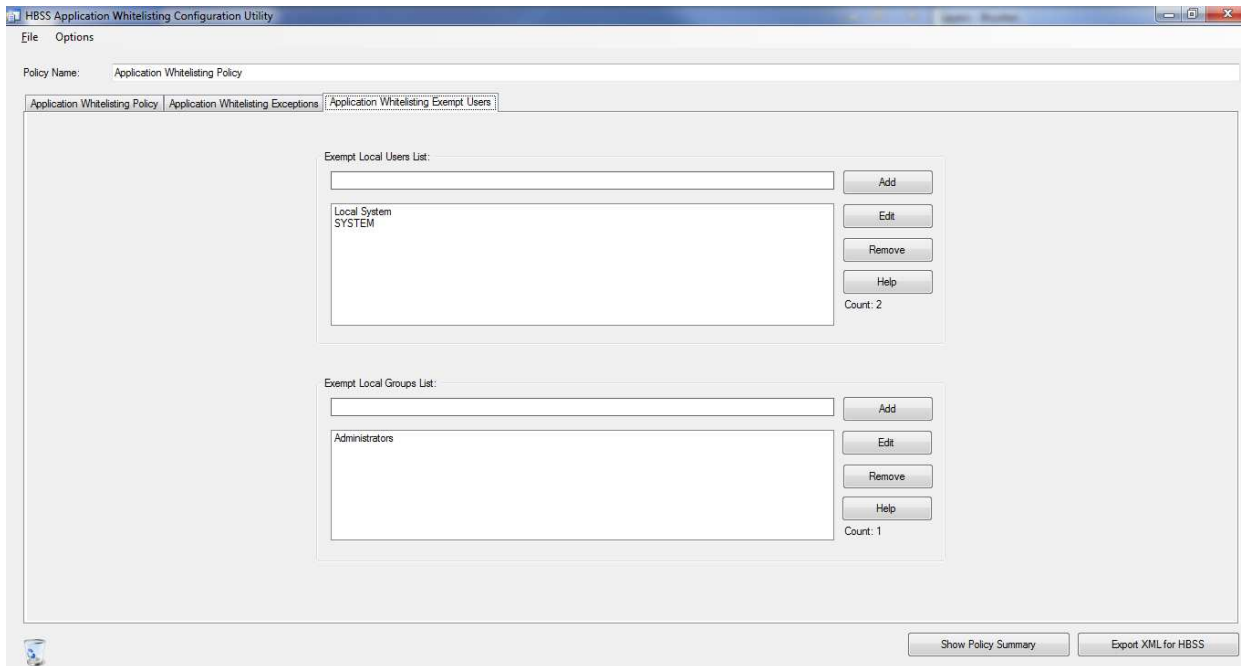
Count: 4

File	Access
\\Local Settings\\Temp\\Gradkell Systems, Inc\\DBsign Data Security Suite\\Temp.Config	Execution
\\Local Settings\\Temp\\Gradkell Systems, Inc\\DBsign Data Security Suite\\Temp.dll	Execution
\\Local Settings\\Temp\\Gradkell Systems, Inc\\DBsign Data Security Suite\\Temp.Manifest	Execution
\\Local Settings\\Temp\\Gradkell Systems, Inc\\DBsign Data Security Suite\\Temp.tmp	Execution

Show Policy Summary Export XML for HBSS

The **Application Whitelisting Exempt Users** tab lists Local Users and Local Groups that should be excluded from the whitelisting rules (e.g., administrators who are authorized to install or update software). You can ignore this tab initially since you will only be monitoring, not blocking, any events that are received.

Consider creating a separate local administrators subgroup that is specifically for installing software and updates to better protect normal administrators performing other sorts of administrative functions. Another option to consider would be to have two separate application whitelisting policies, one without administrator exemptions and one with them. Then, when a workstation needs software installed or updated by an administrator, temporarily apply the policy with the administrator exemptions.



You should now be familiar with the different components of the HIPS application whitelisting tool.

Now perform the following steps:

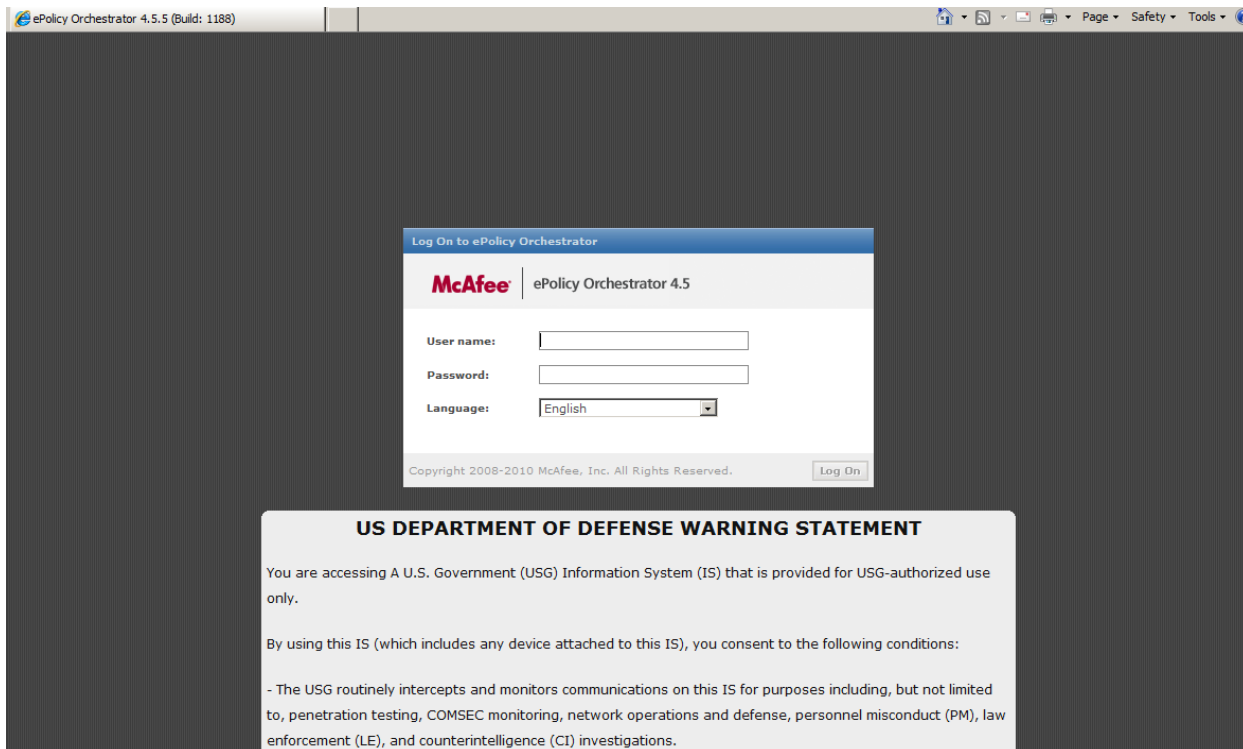
1. Go back to the tab named “Application Whitelisting Policy”
2. Type in a name for your policy in the “Policy Name:” box.
3. Select which version of HIPS your network is running (most networks are running HIPS 7.0)
4. Select the Severity to informational unless logging was selected for another level, if it was, then select that severity level.
5. Save your policy with a unique name. Every time you change the policy, save it with a different name to keep an archive of all your policies over time.
6. At the top of the HIPS application whitelisting tool, click on “File” then “Export XML for HBSS” and export the policy to the desktop.

Importing Policy

Make sure that you have completed the previous 6 steps in the HIPS application whitelisting tool before proceeding any further in this guide:

To import a policy into the ePO server:

Log into the ePO server.



Log On to ePolicy Orchestrator

McAfee | ePolicy Orchestrator 4.5

User name:

Password:

Language:

Copyright 2008-2010 McAfee, Inc. All Rights Reserved.

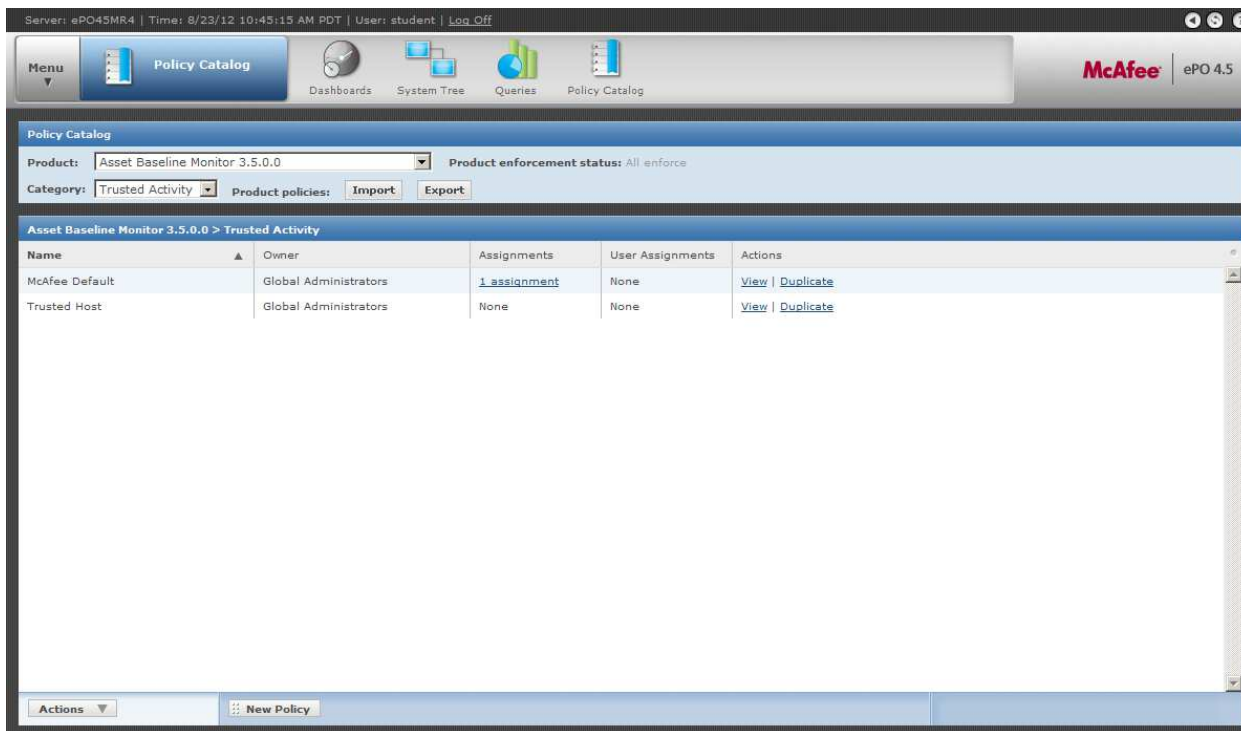
US DEPARTMENT OF DEFENSE WARNING STATEMENT

You are accessing A U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

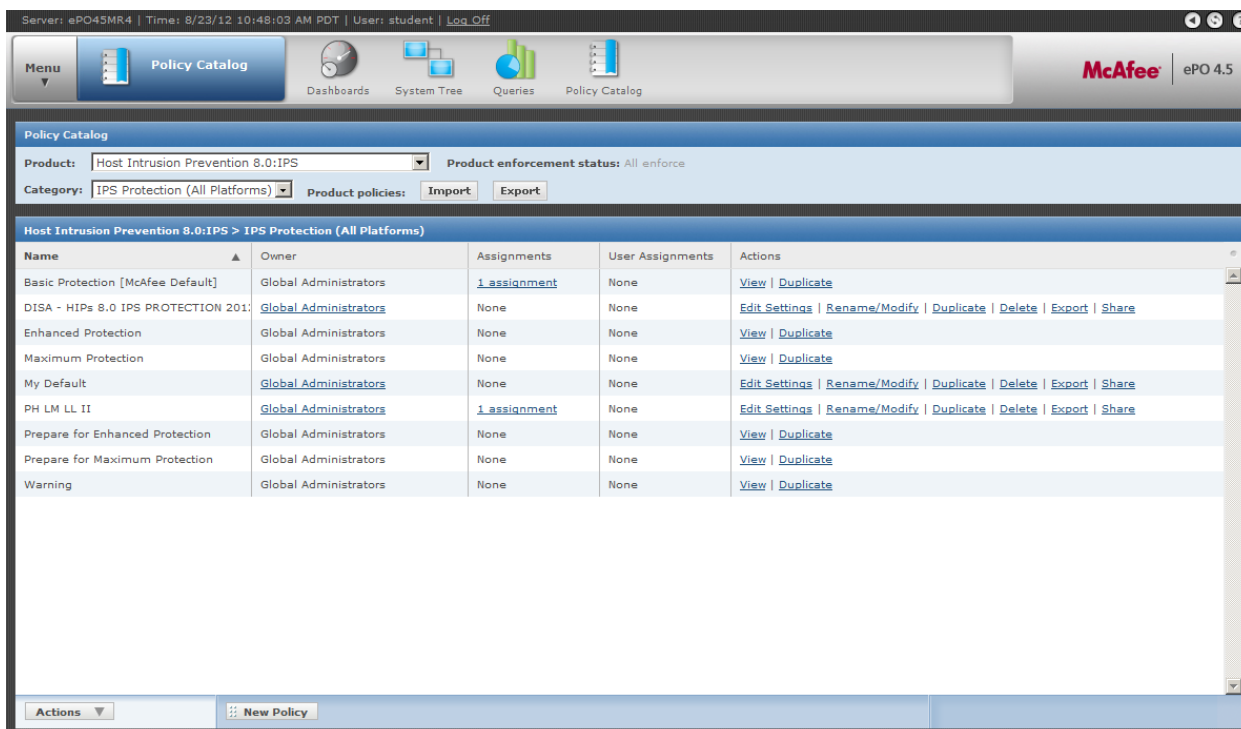
- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

Navigate to the “Policy Catalog” tab.



Select the Correct Version of HIPS in the “Product” dropdown menu (in the example below, we are running HIPS 8). The Name you will select will be similar to “Host Intrusion Prevention 7.0.5:IPS” or “Host Intrusion Prevention 8.0:IPS” depending on which version you are running. It will look like one of the following screens depending on your version:

This is if you are running HIPS 8:



This is if you are running HIPS 7:

Server: ePO45MR4 | Time: 8/23/12 10:50:04 AM PDT | User: student | [Log Off](#)

Menu Policy Catalog Dashboards System Tree Queries Policy Catalog McAfee ePO 4.5

Policy Catalog

Product: Host Intrusion Prevention 7.0.5:IPS Product enforcement status: All enforce

Category: IPS Options (All Platforms) Product policies: Import Export

Host Intrusion Prevention 7.0.5:IPS > IPS Options (All Platforms)

Name	Owner	Assignments	User Assignments	Actions
Adaptive	Global Administrators	None	None	View Duplicate
My Default	Global Administrators	1 assignment	None	Edit Settings Rename/Modify Duplicate Delete Export Share
Off	Global Administrators	None	None	View Duplicate
On [McAfee Default]	Global Administrators	1 assignment	None	View Duplicate

Actions New Policy

Next, regardless of your version, you will select the “IPS Rules (All Platforms)” in the “Category” dropdown menu (which is located below the “Product” dropdown menu)

Server: ePO45MR4 | Time: 8/23/12 10:51:30 AM PDT | User: student | [Log Off](#)

Menu Policy Catalog Dashboards System Tree Queries Policy Catalog McAfee ePO 4.5

Policy Catalog

Product: Host Intrusion Prevention 8.0:IPS Product enforcement status: All enforce

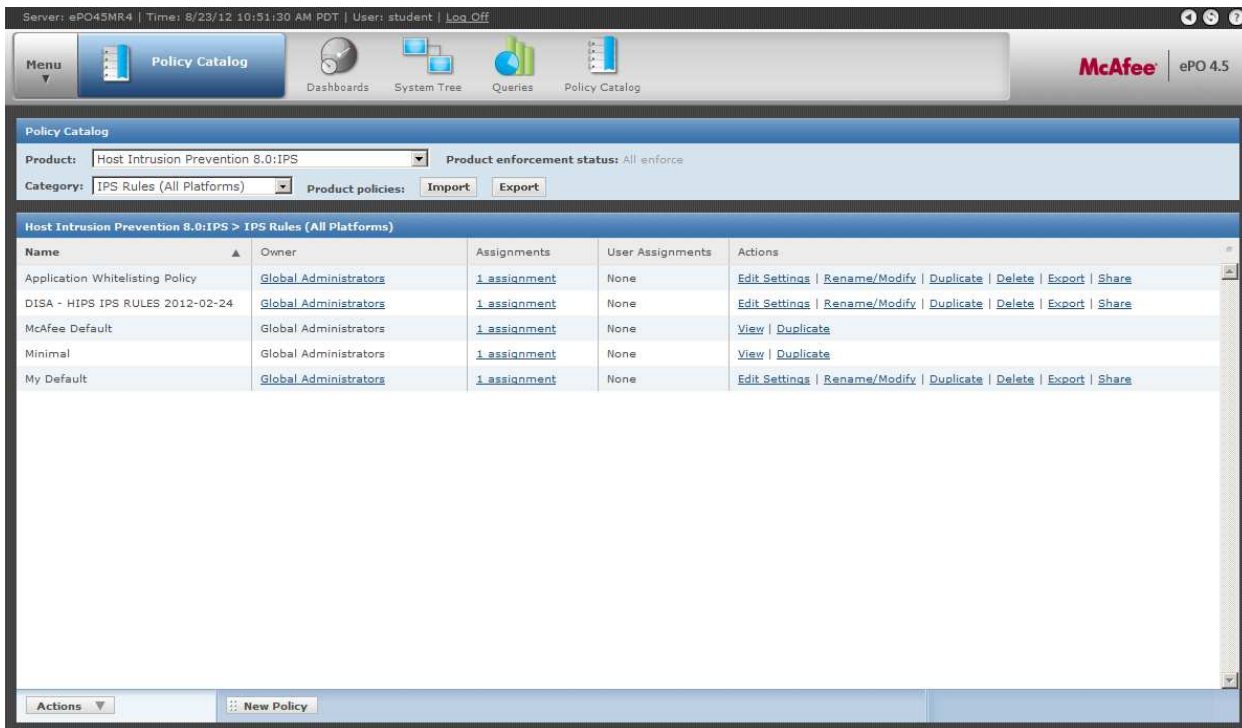
Category: IPS Rules (All Platforms) Product policies: Import Export

Host Intrusion Prevention 8.0:IPS > IPS Rules (All Platforms)

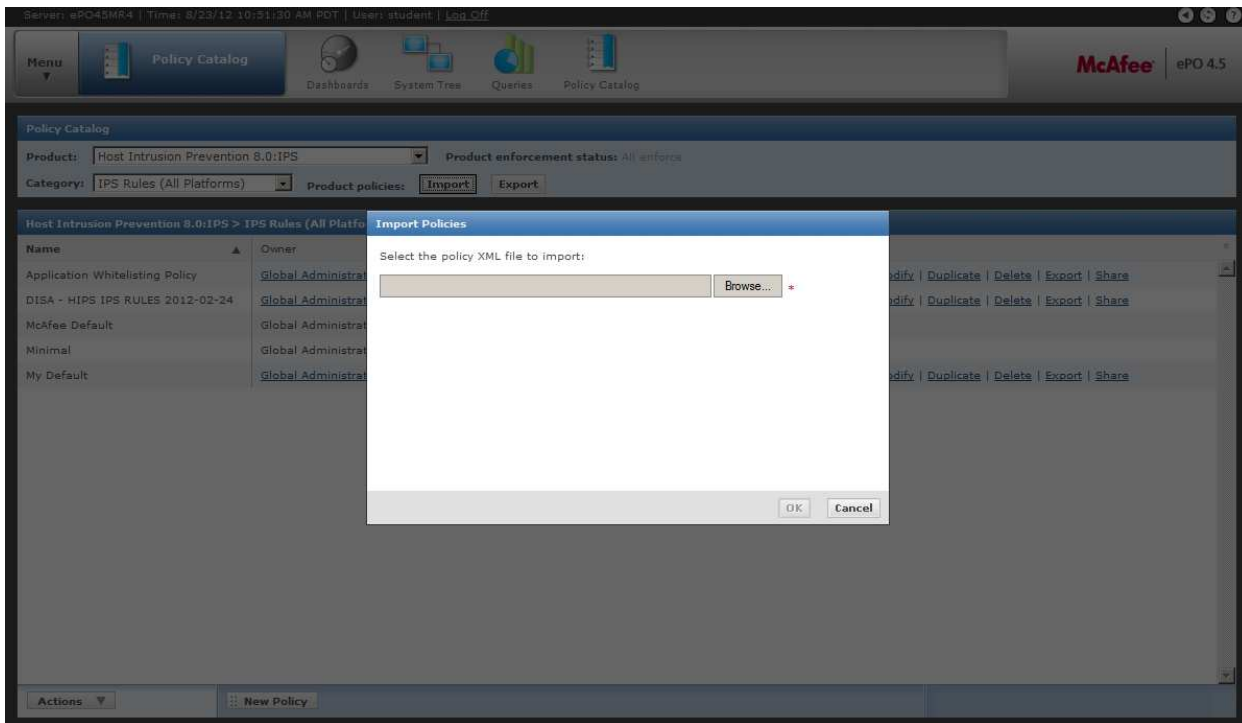
Name	Owner	Assignments	User Assignments	Actions
Application Whitelisting Policy	Global Administrators	1 assignment	None	Edit Settings Rename/Modify Duplicate Delete Export Share
DISA - HIPS IPS RULES 2012-02-24	Global Administrators	1 assignment	None	Edit Settings Rename/Modify Duplicate Delete Export Share
McAfee Default	Global Administrators	1 assignment	None	View Duplicate
Minimal	Global Administrators	1 assignment	None	View Duplicate
My Default	Global Administrators	1 assignment	None	Edit Settings Rename/Modify Duplicate Delete Export Share

Actions New Policy

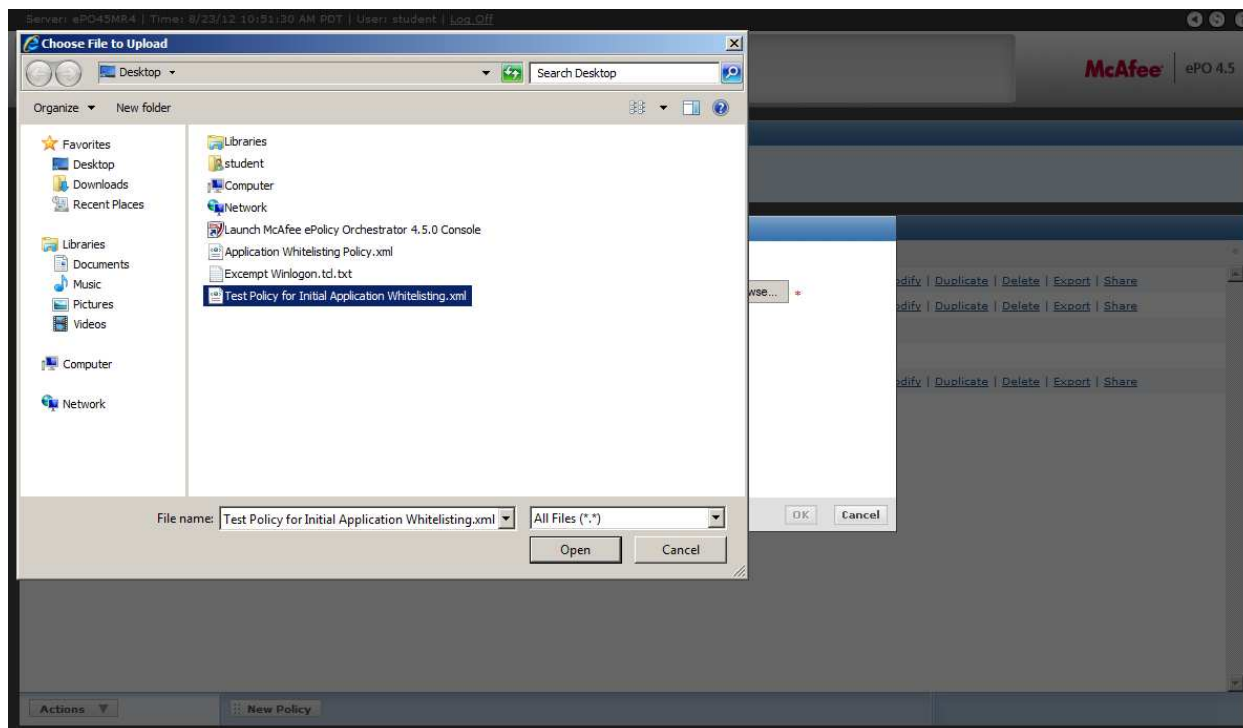
You will see a screen with a list of the currently available HIPS policies on your ePO server. Next Click the “Import” Button, to the right of “Product policies:”.



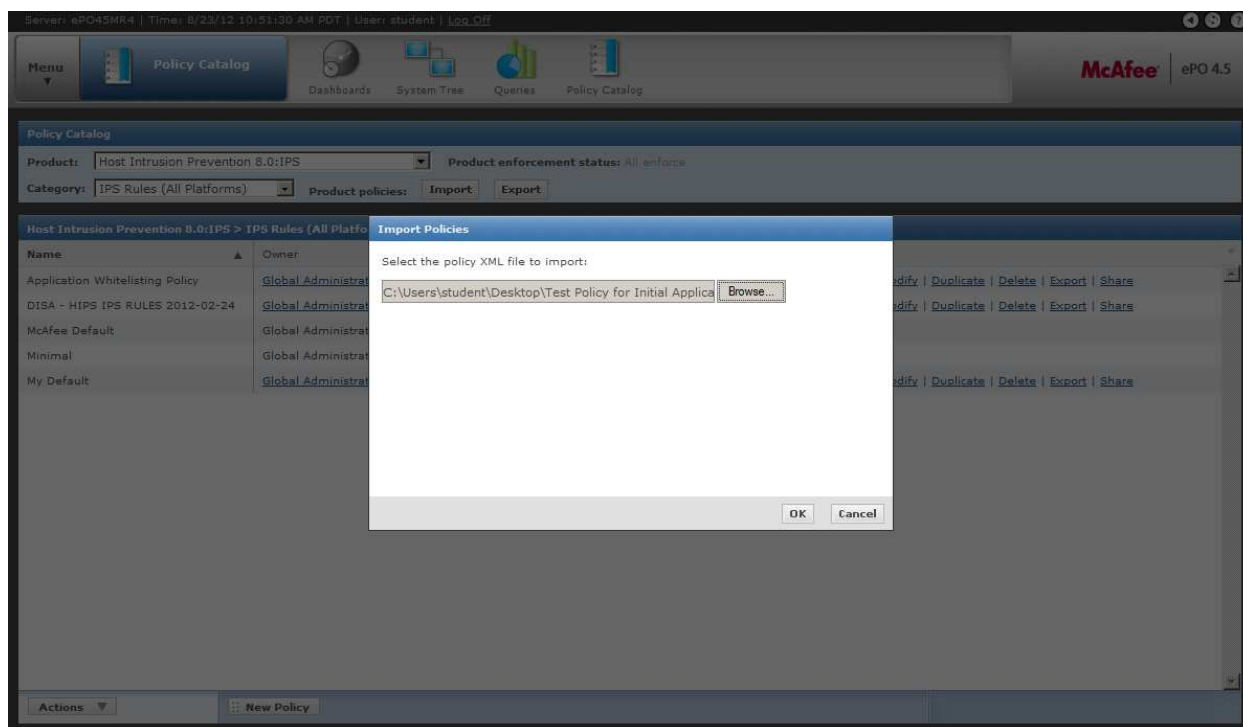
A new window will display as shown: Click “Browse...” to navigate and select the XML policy file you exported from the application whitelisting application.



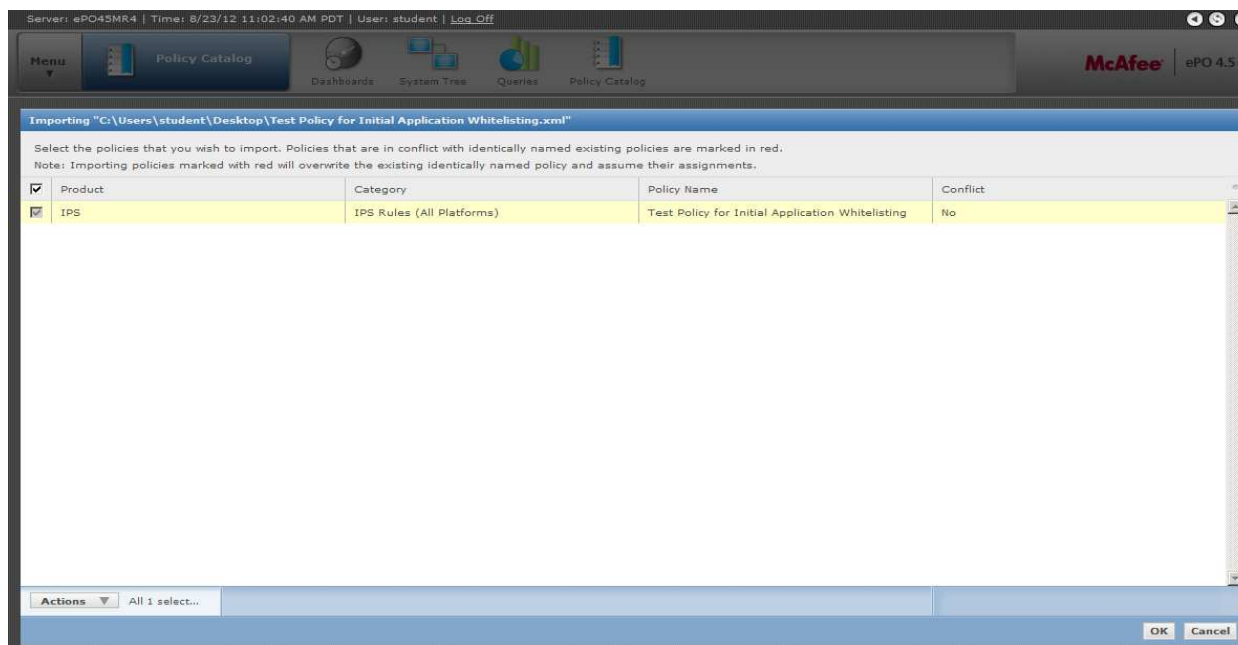
Here is a screenshot of the browse window that pops up when you click the “Browse” button. As you can see, we named our Application Whitelisting policy, “Test Policy for Initial Application Whitelisting”.



Once you click, “Open” the following window will be displayed:

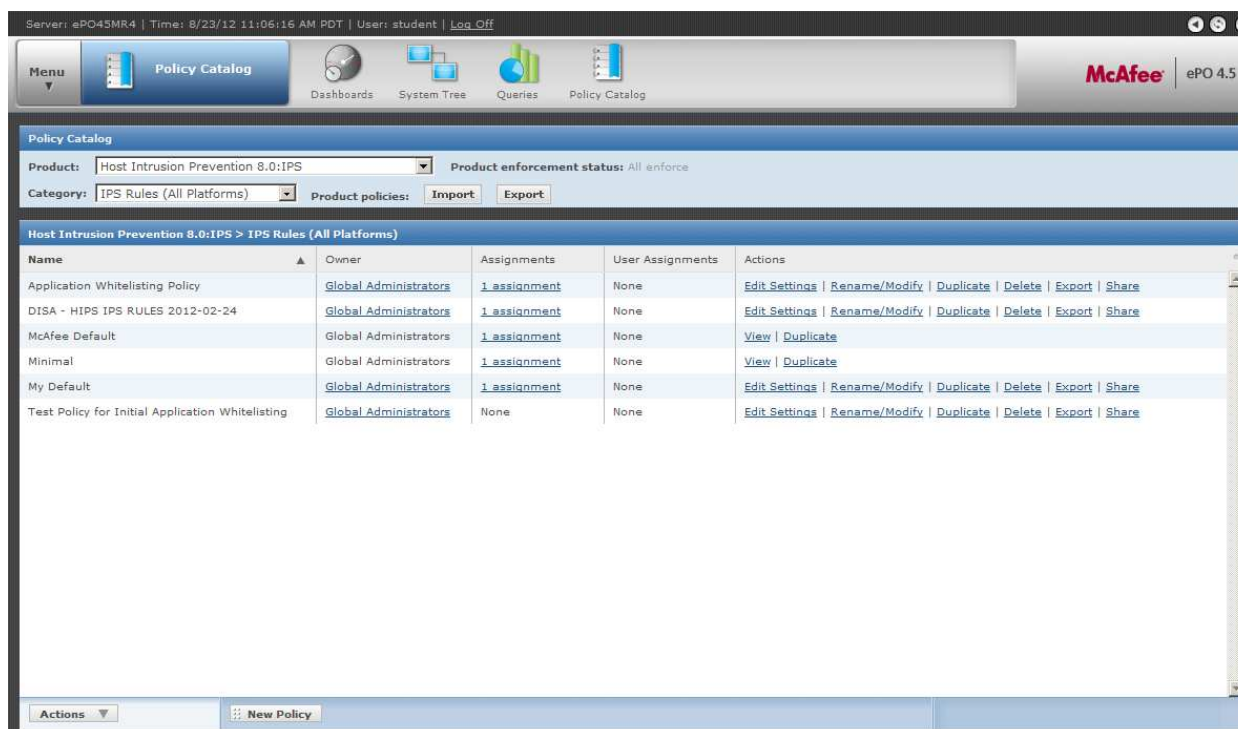


Click “OK” to confirm the policy import. The window below will be displayed:



Make sure the conflict column states "No" for the initial test policy. If the conflict column states "Yes", you will need to go back to the Application Whitelisting tool and rename the policy and repeat the steps above to import the policy with no name conflicts. Later, when you update an existing policy, having a conflict will be appropriate so that the policy within the EPO server will be updated and automatically assigned to the same computers as before.

Click “OK” to confirm the policy import again. You will be brought back to the main HIPS policy screen. Make sure your policy name is now in the list. If it is, you have successfully imported the new policy.

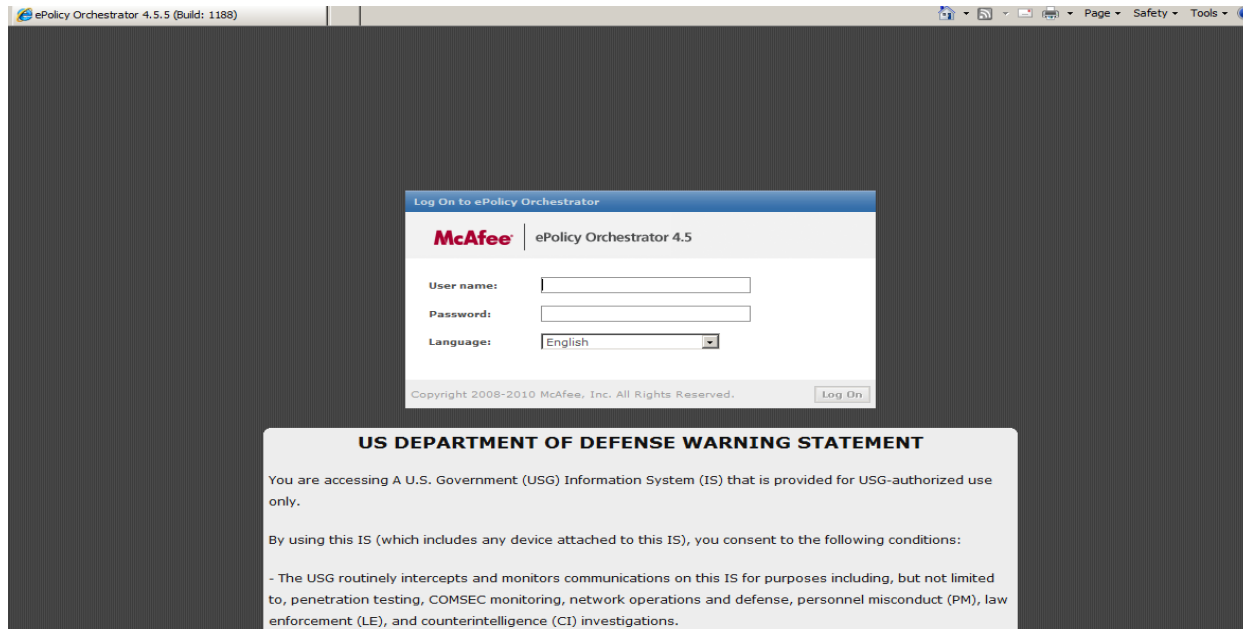


If you do not see your policy in the list, make sure you have navigated to the correct “Product:” and “Category:” sections. Make sure you have rights to import policies, and make sure you are not using a duplicate name which causes a policy conflict.

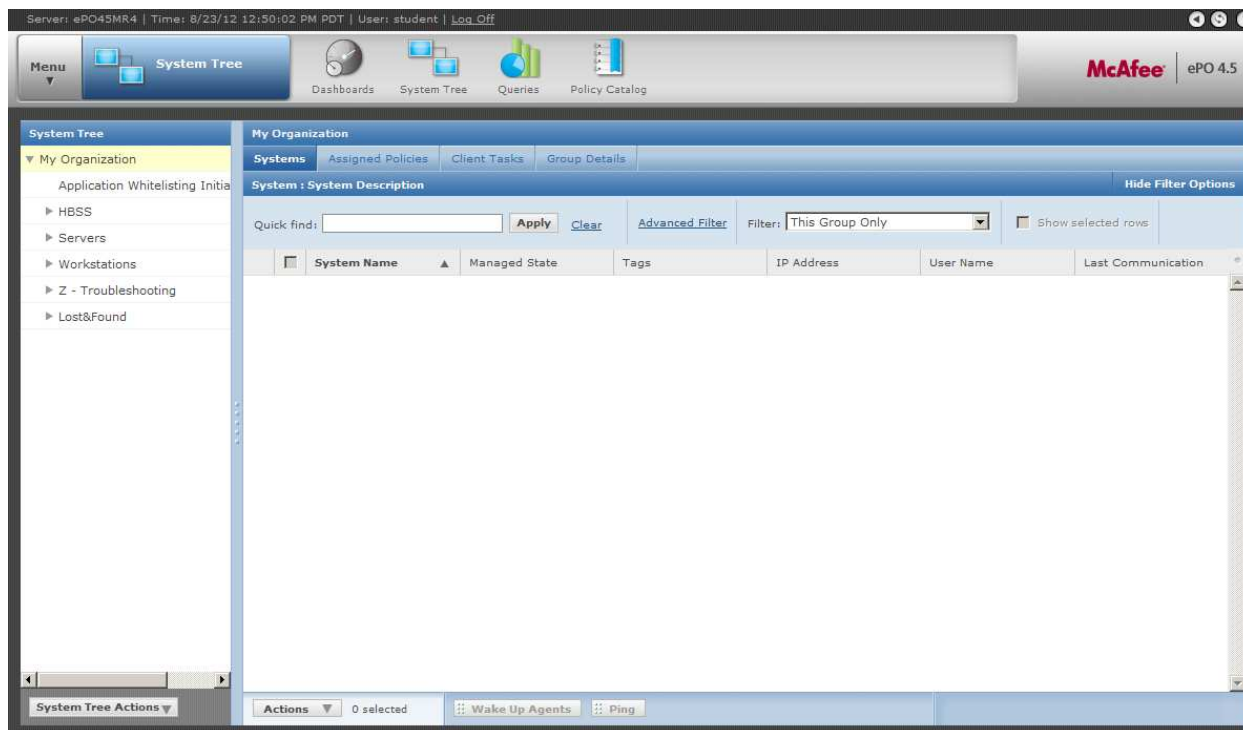
You have now successfully imported your initial application whitelisting policy!

Applying application whitelisting policies to your test group

Log into the ePO server.



Navigate to the “System Tree” Tab.



Select the container you previously selected or created for the Application Whitelisting test machines. In our case, this container is called, “Application Whitelisting Initial Test Group”. Selecting the container will display the machines in that container. Make sure that all of your test machines are in the test container.

Server: ePO45MR4 | Time: 8/23/12 12:50:02 PM PDT | User: student | [Log Off](#)

Menu System Tree Dashboards System Tree Queries Policy Catalog

McAfee ePO 4.5

System Tree

- My Organization
 - Application Whitelisting Initial Test Group
 - HBSS
 - Servers
 - Workstations
 - Windows 7
 - Windows XP
 - Z - Troubleshooting
 - Lost&Found

My Organization > Application Whitelisting Initial Test Group

Systems Assigned Policies Client Tasks Group Details

System : System Description

Quick find: [Apply](#) [Clear](#) [Advanced Filter](#) Filters: This Group and All Subgroups [Hide Filter Options](#) ☐ Show selected rows

<input type="checkbox"/>	System Name	Managed State	Tags	IP Address	User Name	Last Communication
<input type="checkbox"/>	WIN7CLIENT64	Managed	Workstation	192.168.10.100	student	8/22/12 3:12:42 PM
<input type="checkbox"/>	WIN7CLIENT86	Managed	Install HIPS, Worksta	192.168.10.101	N/A	8/21/12 10:49:02 AM
<input type="checkbox"/>	WINXPCLIENT86	Managed	Workstation	192.168.10.102	N/A	8/23/12 12:19:09 PM

System Tree Actions

Actions 0 selected [Wake Up Agents](#) [Ping](#)

With your test container selected, click on the “Assigned Policies” Tab. This will bring up the policies assigned to your test container. You should see the window below.

Server: ePO45MR4 | Time: 8/23/12 12:50:02 PM PDT | User: student | [Log Off](#)

Menu System Tree Dashboards System Tree Queries Policy Catalog

McAfee ePO 4.5

System Tree

- My Organization
 - Application Whitelisting Initial Test Group
 - HBSS
 - Servers
 - Workstations
 - Windows 7
 - Windows XP
 - Z - Troubleshooting
 - Lost&Found

My Organization > Application Whitelisting Initial Test Group

Systems **Assigned Policies** Client Tasks Group Details

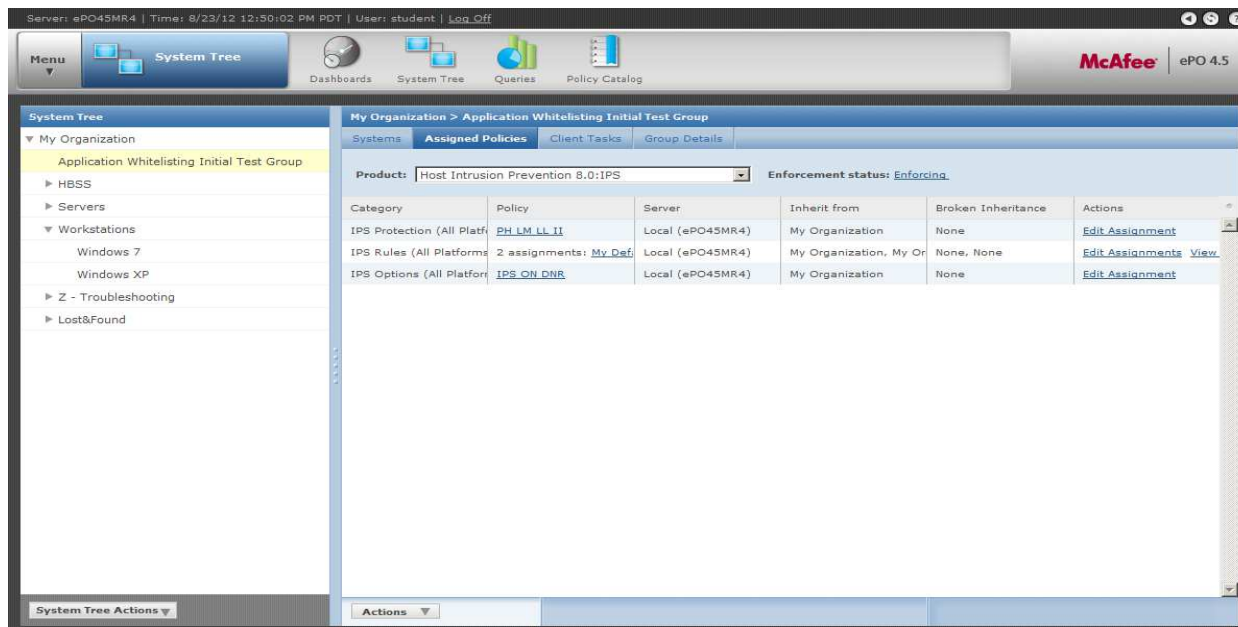
Products: Asset Baseline Monitor 3.5.0.0 Enforcement status: [Enforcing](#)

Category	Policy	Server	Inherit from	Broken Inheritance	Actions
Trusted Activity	McAfee Default	Local (ePO45MR4)	Global Root	None	Edit Assignment
File Permissions	My Default	Local (ePO45MR4)	My Organization	None	Edit Assignment
Registry Monitor	My Default	Local (ePO45MR4)	My Organization	None	Edit Assignment

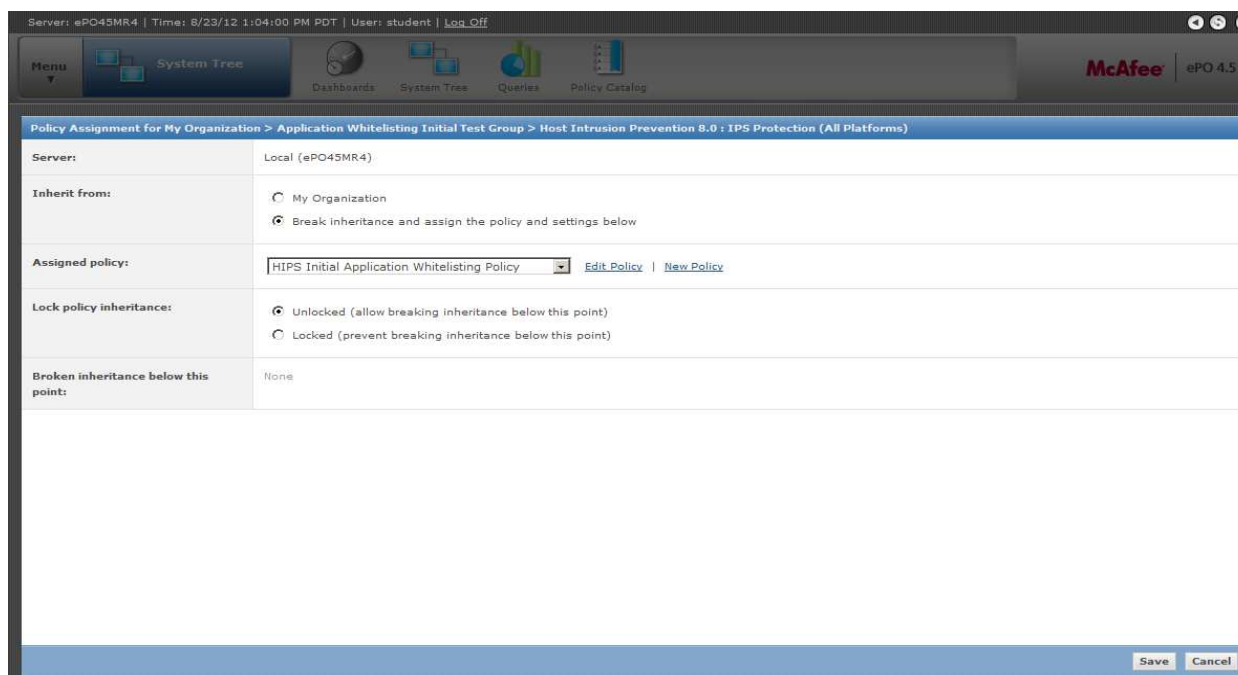
System Tree Actions

Actions

In the “Product” dropdown Menu, select the version of HIPS you are running (7 or 8) IPS policy list. The screen will look as follows. Your display may look slightly different if you are navigating to the HIPS 7 module in the “Product” dropdown menu.

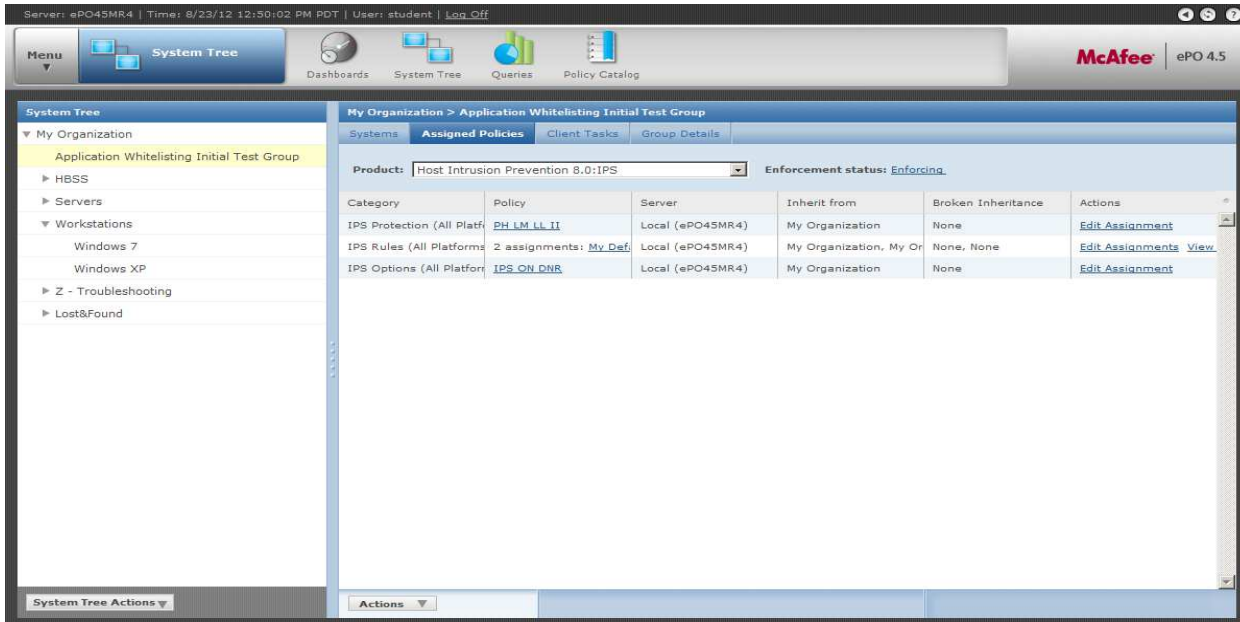


In the “Category” column, find the entry that says, “IPS Protection (All Platforms)”, click “Edit Assignments” to edit the IPS Protection policy that are assigned to your test containers. Next change the currently applied policy to be the IPS Protection Policy that you created. Make sure to select the “Break Inheritance and assign the policy and setting below” radio button and that you select your Application Whitelisting HIPS Protection Policy from the “Assigned policy:” menu dropdown. Select the “Unlocked (Allow breaking inheritance beyond this point)” option as well. Click Save to apply your HIPS protection policy to your application whitelisting test container.



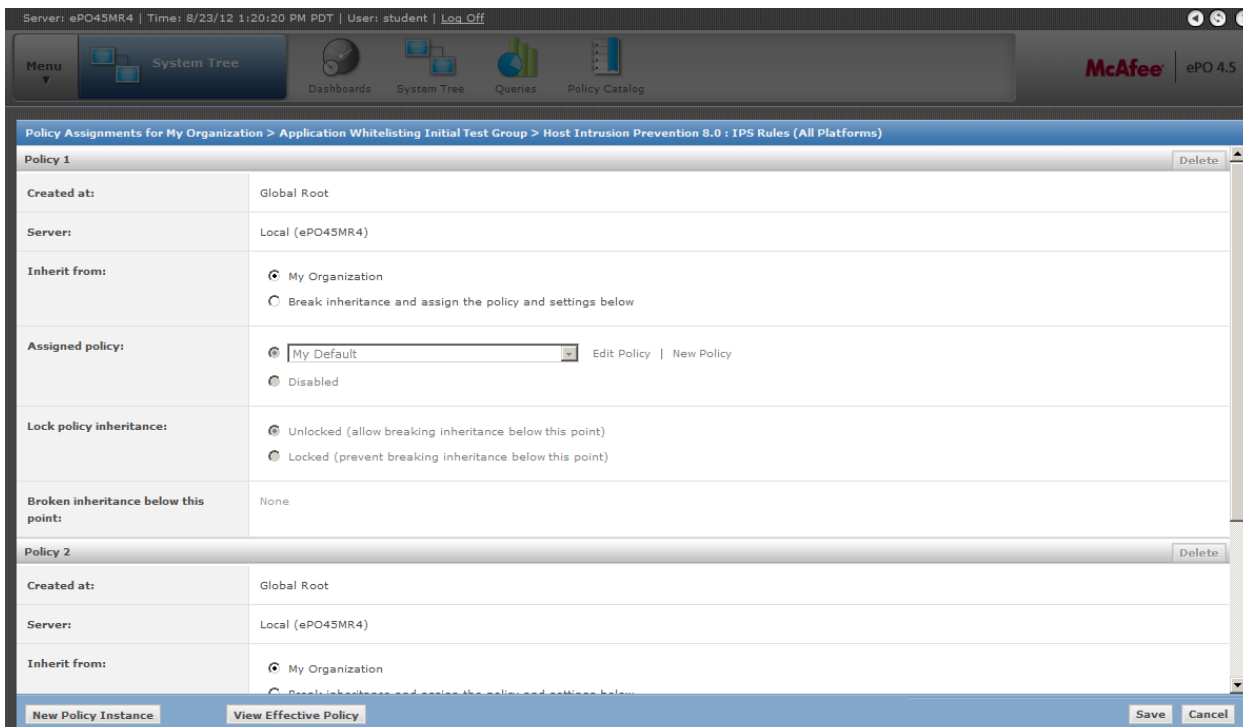
Next we will assign the IPS Rule Policy that contains the Application Whitelisting Rules to your test container.

With your test container selected, click on the “Assigned Policies” Tab. This will bring up the policies assigned to your test container. You should see the window below.



In the “Product” dropdown menu, select the version of HIPS you are running (7 or 8) IPS policy list. The screen will look as follows. Your display may look slightly different if you are navigating to the HIPS 7 module in the “Product” dropdown menu. In the “Category” column, find the entry that says, “IPS Rules (All Platforms)”, click “Edit Assignments” to edit the IPS Rules policies that are assigned to your test containers.

The following screen will be displayed once you click the “Edit Assignments”:



Click “New Policy Instance” to create a new section to make a new policy assignment. The new section will be appended to the end of the current assignments. (Watch the scroll bar).

Server: ePO45MR4 | Time: 8/23/12 1:27:42 PM PDT | User: student | [Log Off](#)

Menu System Tree Dashboards System Tree Queries Policy Catalog

McAfee ePO 4.5

Policy Assignments for My Organization > Application Whitelisting Initial Test Group > Host Intrusion Prevention 8.0 : IPS Rules (All Platforms)

Inherit from:
☒ My Organization
☐ Break inheritance and assign the policy and settings below

Assigned policy:
☒ DISA - HIPS IPS RULES 2012-02-24 [Edit Policy](#) [New Policy](#)
☐ Disabled

Lock policy inheritance:
☒ Unlocked (allow breaking inheritance below this point)
☐ Locked (prevent breaking inheritance below this point)

Broken inheritance below this point: None

Created at: This Node

Server:

Assigned policy:
☐ Application Whitelisting Policy [Edit Policy](#) [New Policy](#)
☒ Disabled

Lock policy inheritance:
☒ Unlocked (allow breaking inheritance below this point)
☐ Locked (prevent breaking inheritance below this point)

[New Policy Instance](#) [View Effective Policy](#) [Save](#) [Cancel](#)

Now assign the IPS Rules Policy you created by clicking the Assigned policy radio button and selecting your policy name. Make sure the radio button “Unlocked (allow breaking inheritance below this point)” is also selected.

After selecting the appropriate policy your window will look similar to:

Server: ePO45MR4 | Time: 8/23/12 1:27:42 PM PDT | User: student | [Log Off](#)

Menu System Tree Dashboards System Tree Queries Policy Catalog

McAfee ePO 4.5

Policy Assignments for My Organization > Application Whitelisting Initial Test Group > Host Intrusion Prevention 8.0 : IPS Rules (All Platforms)

Inherit from:
☒ My Organization
☐ Break inheritance and assign the policy and settings below

Assigned policy:
☒ DISA - HIPS IPS RULES 2012-02-24 [Edit Policy](#) [New Policy](#)
☐ Disabled

Lock policy inheritance:
☒ Unlocked (allow breaking inheritance below this point)
☐ Locked (prevent breaking inheritance below this point)

Broken inheritance below this point: None

Created at: This Node

Server:

Assigned policy:
☒ Test Policy for Initial Application Whitelisting [Edit Policy](#) [New Policy](#)
☐ Disabled

Lock policy inheritance:
☒ Unlocked (allow breaking inheritance below this point)
☐ Locked (prevent breaking inheritance below this point)

[New Policy Instance](#) [View Effective Policy](#) [Save](#) [Cancel](#)

Click Save to apply your policy to your test group on the ePO server. Congratulations, you have successfully applied your initial Application Whitelisting policies.

Updating clients with the new policy

Log into the ePO server:

Log On to ePolicy Orchestrator

McAfee | ePolicy Orchestrator 4.5

User name:

Password:

Language:

Copyright 2008-2010 McAfee, Inc. All Rights Reserved.

US DEPARTMENT OF DEFENSE WARNING STATEMENT

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

Navigate to the “System Tree” Tab:

Server: ePO45MR4 | Time: 8/23/12 2:38:45 PM PDT | User: student | [Log Off](#)

Menu **System Tree** Dashboards System Tree Queries Policy Catalog

McAfee | ePO 4.5

System Tree

My Organization

Application Whitelisting Initial

- HBSS
- Servers
- Workstations
 - Windows 7
 - Windows XP
- Z - Troubleshooting
- Lost&Found

My Organization

Systems Assigned Policies Client Tasks Group Details

System : System Description

Quick find: Filter: ☐ Show selected rows

<input type="checkbox"/>	System Name	Managed State	Tags	IP Address	User Name	Last Communication
<input type="checkbox"/>	EPO45MR4	Managed	Install HIPS, Server	192.168.10.10	student	8/23/12 1:59:07 PM
<input type="checkbox"/>	WIN2K8R2-DC1	Managed	Server	192.168.10.5	N/A	8/23/12 1:40:07 PM
<input type="checkbox"/>	WIN7CLIENT64	Managed	Workstation	192.168.10.100	student	8/22/12 3:12:42 PM
<input type="checkbox"/>	WIN7CLIENT86	Managed	Install HIPS, Workstation	192.168.10.101	N/A	8/21/12 10:49:02 AM
<input type="checkbox"/>	WINXPCLIENT86	Managed	Workstation	192.168.10.102	student	8/23/12 2:32:50 PM

System Tree Actions 0 selected

Select your test Application Whitelisting container:

Server: ePO45MR4 | Time: 8/23/12 2:38:45 PM PDT | User: student | [Log Off](#)

Menu System Tree Dashboards System Tree Queries Policy Catalog

McAfee ePO 4.5

System Tree

My Organization > Application Whitelisting Initial Test Group

Systems Assigned Policies Client Tasks Group Details

System : System Description

Quick find: Apply Clear Advanced Filter Filter: This Group and All Subgroups Show selected rows

<input type="checkbox"/>	System Name	Managed State	Tags	IP Address	User Name	Last Communication
<input type="checkbox"/>	WIN7CLIENT64	Managed	Workstation	192.168.10.100	student	8/22/12 3:12:42 PM
<input type="checkbox"/>	WIN7CLIENT86	Managed	Install HIPS, Workstation	192.168.10.101	N/A	8/21/12 10:49:02 AM
<input type="checkbox"/>	WINXPCLIENT86	Managed	Workstation	192.168.10.102	student	8/23/12 2:32:50 PM

System Tree Actions 0 selected Wake Up Agents Ping

Select all the machines in the container by clicking the check box in the column headings. This will select all machines in the list.

Server: ePO45MR4 | Time: 8/23/12 2:38:45 PM PDT | User: student | [Log Off](#)

Menu System Tree Dashboards System Tree Queries Policy Catalog

McAfee ePO 4.5

System Tree

My Organization > Application Whitelisting Initial Test Group

Systems Assigned Policies Client Tasks Group Details

System : System Description

Quick find: Apply Clear Advanced Filter Filter: This Group and All Subgroups Show selected rows

<input checked="" type="checkbox"/>	System Name	Managed State	Tags	IP Address	User Name	Last Communication
<input checked="" type="checkbox"/>	WIN7CLIENT64	Managed	Workstation	192.168.10.100	student	8/22/12 3:12:42 PM
<input checked="" type="checkbox"/>	WIN7CLIENT86	Managed	Install HIPS, Workstation	192.168.10.101	N/A	8/21/12 10:49:02 AM
<input checked="" type="checkbox"/>	WINXPCLIENT86	Managed	Workstation	192.168.10.102	student	8/23/12 2:32:50 PM

System Tree Actions All 3 select... Wake Up Agents Ping

Click the “Wake Up Agents” Button. The screen below will be displayed:

Server: ePO45MR4 | Time: 8/23/12 2:41:34 PM PDT | User: student | [Log Off](#)

Menu System Tree Dashboards System Tree Queries Policy Catalog McAfee ePO 4.5

Wake Up McAfee Agent

Click "OK" to send the wake-up call to the target systems. To see the status of the wake-up call, go to the Server Task Log.

Target systems:	WIN7CLIENT64, WIN7CLIENT86, WINXPCLIENT86
Wake-up call type:	<input checked="" type="radio"/> Agent Wake-Up Call <input type="radio"/> SuperAgent Wake-Up Call
Randomization:	<input type="text" value="0"/> minutes
Options:	<input checked="" type="checkbox"/> Get full product properties in addition to system properties. If unchecked, only minimal product properties and system properties are sent.
Force policy update:	<input type="checkbox"/> Force complete policy and task update
Number of attempts:	<input type="text" value="0"/> (Enter 0 for continuous attempts.)
Retry interval:	<input type="text" value="30"/> seconds
Abort after:	<input type="text" value="5"/> minutes
Connect using:	<input checked="" type="radio"/> Last Connected Agent Handler <input type="radio"/> All Agent Handlers

OK Close

Click the “Force complete policy and task update” button. This will push your policies to all of your test machines.

Server: ePO45MR4 | Time: 8/23/12 2:41:34 PM PDT | User: student | [Log Off](#)

Menu System Tree Dashboards System Tree Queries Policy Catalog McAfee ePO 4.5

Wake Up McAfee Agent

Click "OK" to send the wake-up call to the target systems. To see the status of the wake-up call, go to the Server Task Log.

Target systems:	WIN7CLIENT64, WIN7CLIENT86, WINXPCLIENT86
Wake-up call type:	<input checked="" type="radio"/> Agent Wake-Up Call <input type="radio"/> SuperAgent Wake-Up Call
Randomization:	<input type="text" value="0"/> minutes
Options:	<input checked="" type="checkbox"/> Get full product properties in addition to system properties. If unchecked, only minimal product properties and system properties are sent.
Force policy update:	<input checked="" type="checkbox"/> Force complete policy and task update
Number of attempts:	<input type="text" value="0"/> (Enter 0 for continuous attempts.)
Retry interval:	<input type="text" value="30"/> seconds
Abort after:	<input type="text" value="5"/> minutes
Connect using:	<input checked="" type="radio"/> Last Connected Agent Handler <input type="radio"/> All Agent Handlers

OK Close

Click OK to update your test machines with the new policy. This will take you back to the system tree screen. You are finished updating your test machines with the new policy. Wait approximately 5 to 10 minutes to ensure that all hosts have had time to receive and apply the new policy.

It may take a while (possibly even days) to product Application Whitelisting events depending on the actual user activity on the test machines.

Reviewing Logs

In this section you will generate queries and analyze data that is generated from the auditing step.

Querying for Events

This section will show you how to build a sample query on your ePO server to display the application whitelisting events being reported from your test machines. We will also go over interpreting the query results.

Log onto the ePO server

Log On to ePolicy Orchestrator

McAfee | ePolicy Orchestrator 4.5

User name:

Password:

Language:

Copyright 2008-2010 McAfee, Inc. All Rights Reserved.

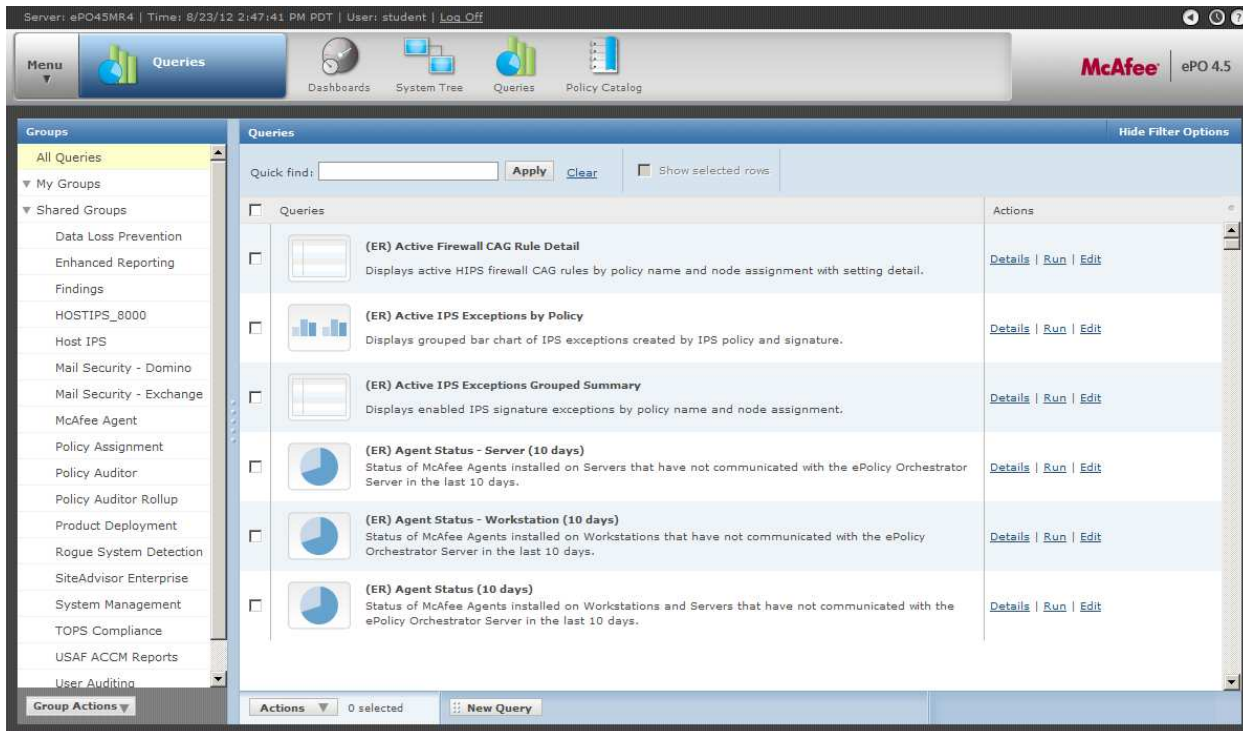
US DEPARTMENT OF DEFENSE WARNING STATEMENT

You are accessing A U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

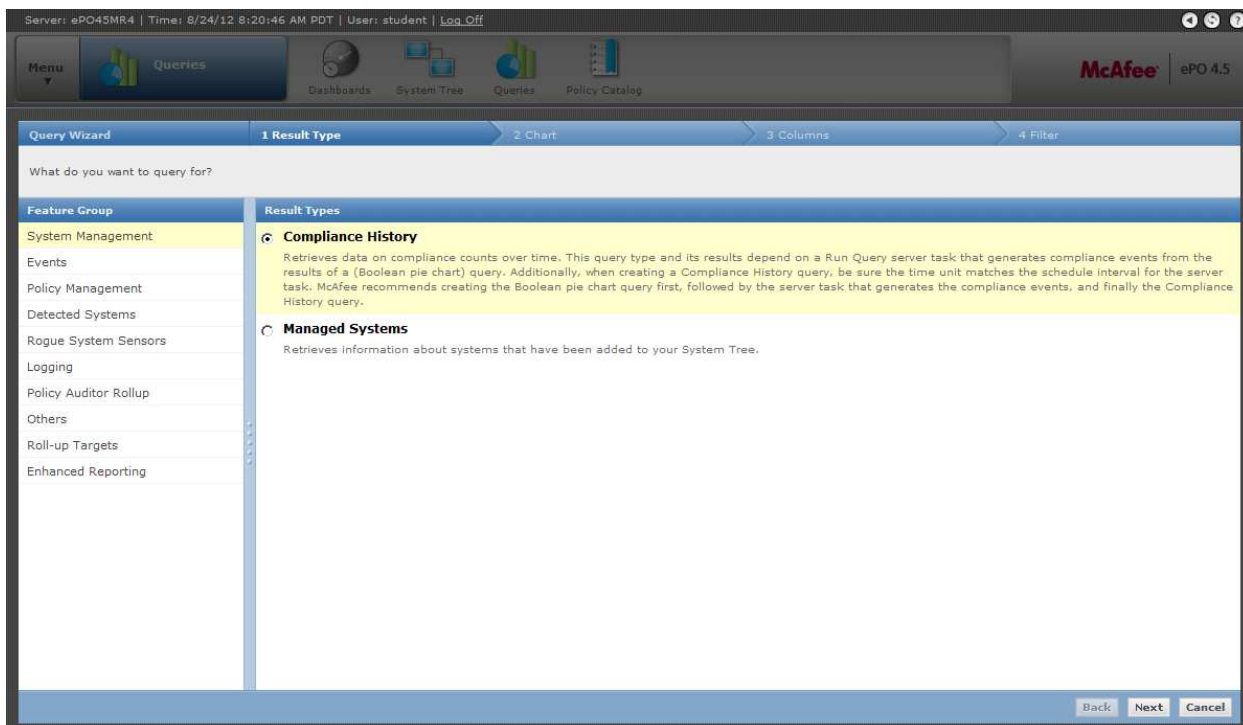
By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

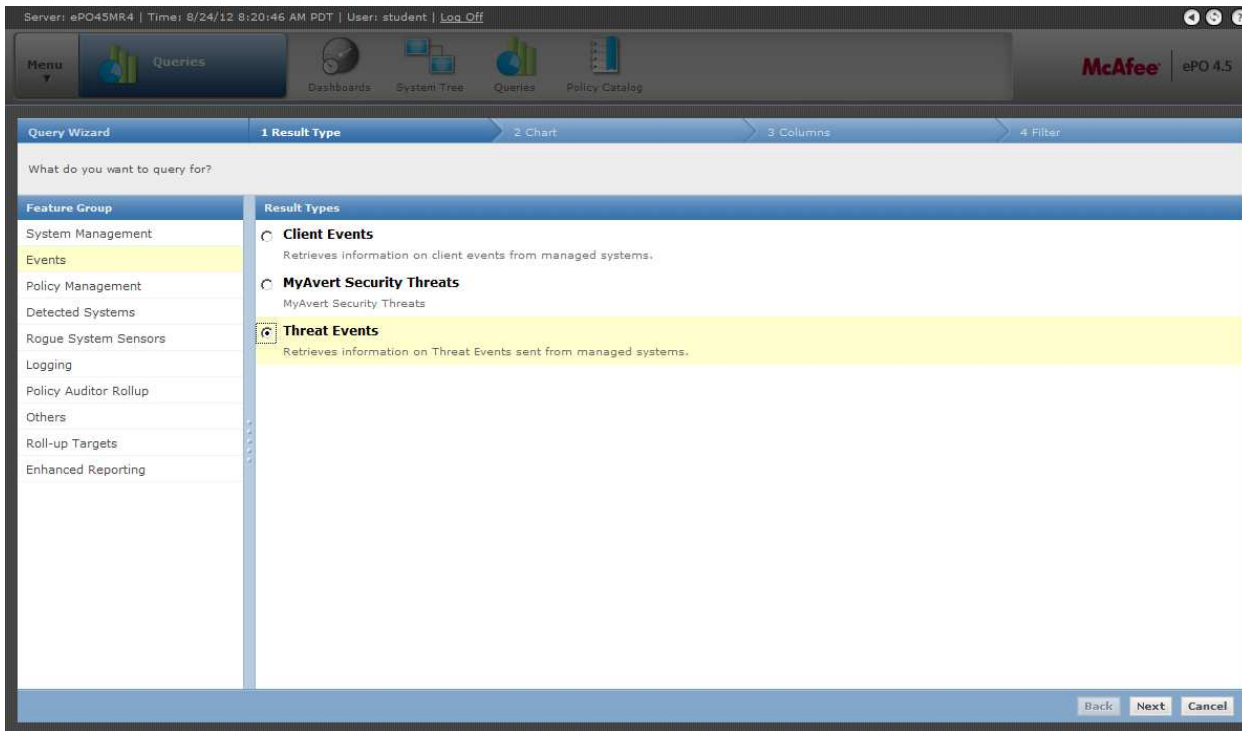
Navigate to the queries tab



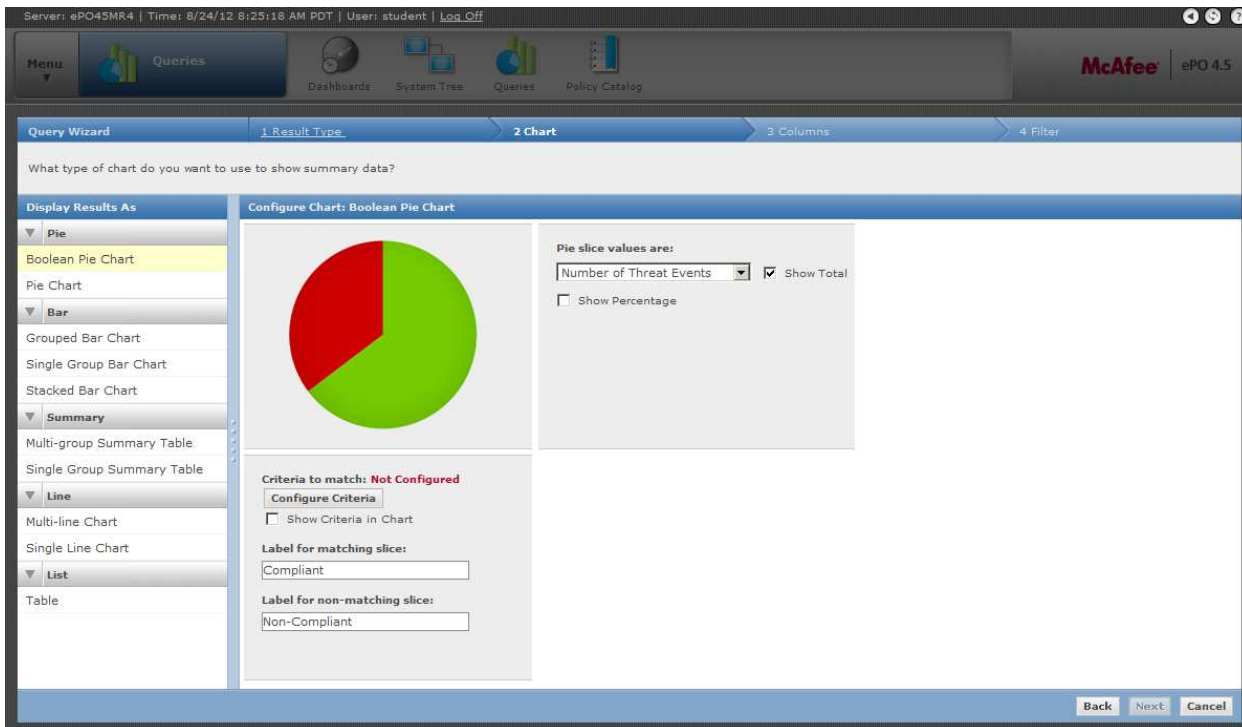
Click “New Query” to create a new query. This is the screen you will see once you click, “New Query”.



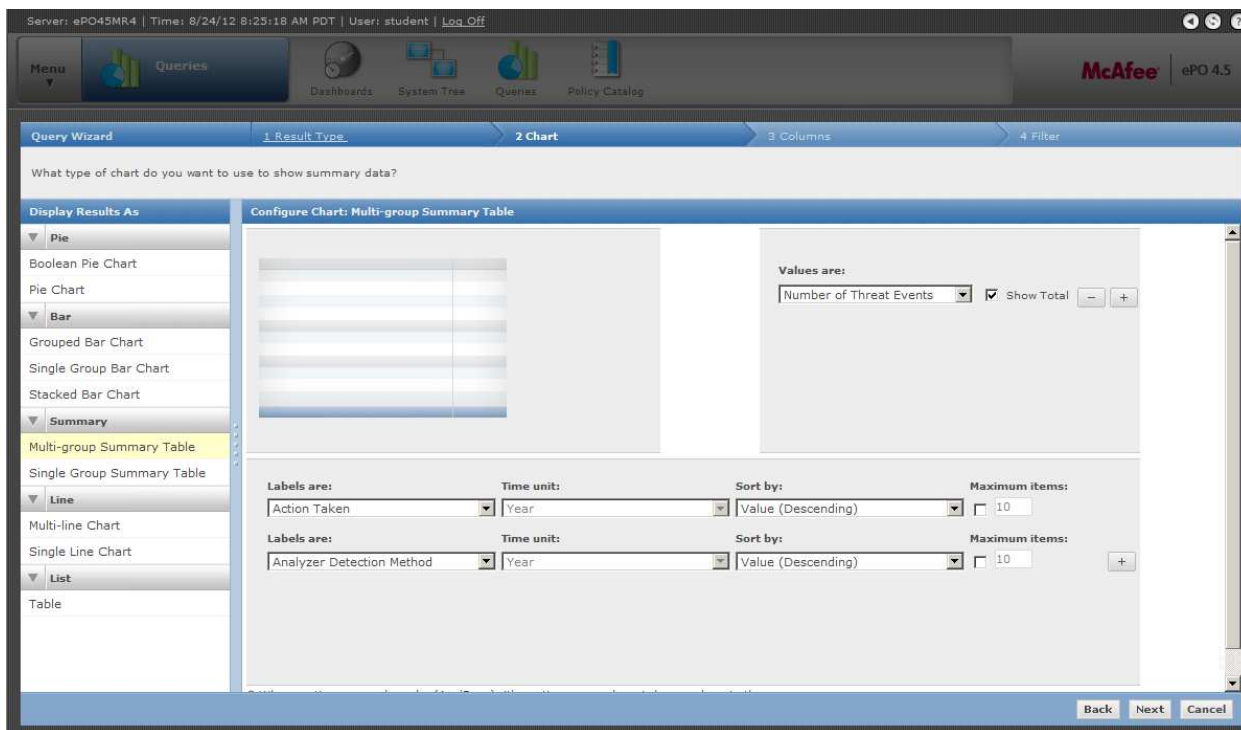
Now navigate to the “Events” then to “Threat Events”. Click “Next”.



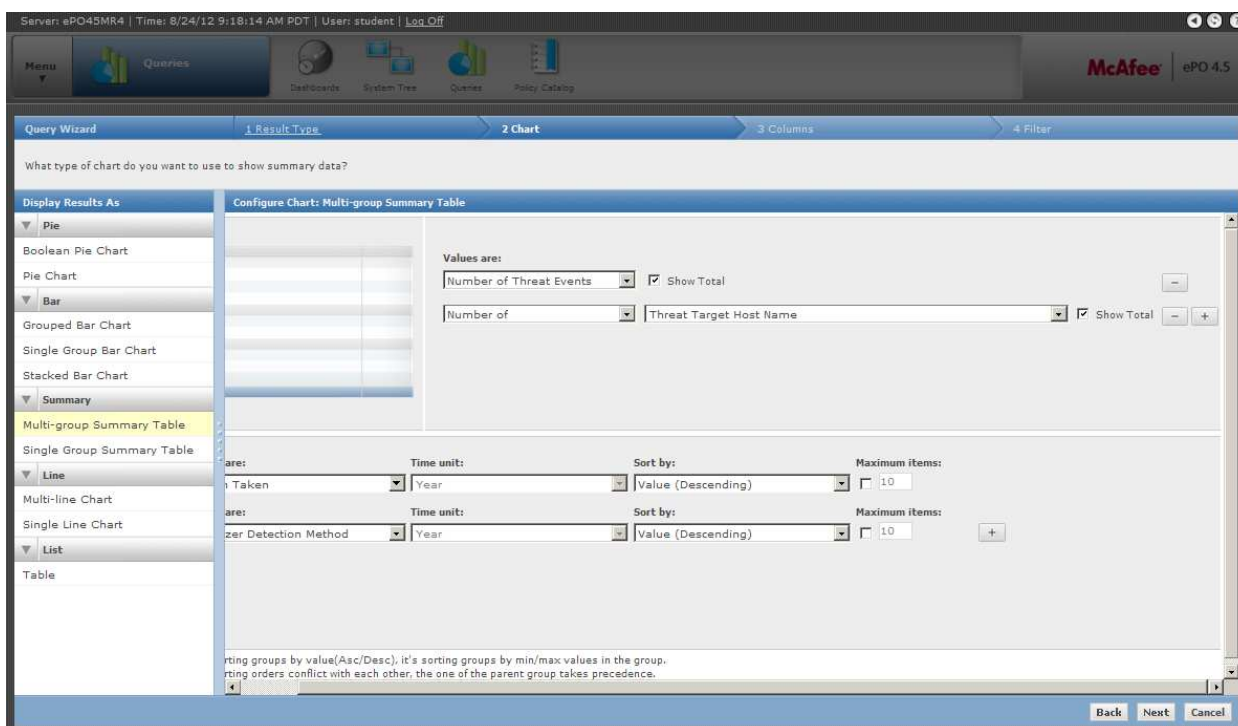
The screen below will be displayed:



Modify this tab, “2 Chart”, and change the “Display Results As” to “Multi-group Summary Table”.



Now configure the “Values are:” portion of the “2 Chart” tab, to “Number of Threat Events”, check the “Show Total” checkbox. Then click the “+” box to add another row. In the new row select “Number of” from the “Values are:” dropdown, select “Threat Target Host Name” then select the “Show Total” checkbox on the right. After completing these steps, your screen will look as follows:



Next configure the “Labels are” options toward the bottom. Select the following fields:

Server: ePO45MR4 | Time: 8/24/12 9:21:11 AM PDT | User: student | Log Off

Menu Queries Dashboards System Test Queries Policy Catalog

McAfee ePO 4.5

Query Wizard 1 Result Type 2 Chart 3 Columns 4 Filter

What type of chart do you want to use to show summary data?

Display Results As

- Pie
 - Boolean Pie Chart
 - Pie Chart
- Bar
 - Grouped Bar Chart
 - Single Group Bar Chart
 - Stacked Bar Chart
- Summary
 - Multi-group Summary Table
 - Single Group Summary Table
- Line
 - Multi-line Chart
 - Single Line Chart
- List
 - Table

Configure Chart: Multi-group Summary Table

Values are:

Number of Threat Events	<input checked="" type="checkbox"/> Show Total
Number of Threat Target Host Name	<input checked="" type="checkbox"/> Show Total

Labels are:

Signature Name (Host IPS)	Time unit: Year	Sort by: Value (Descending)	Maximum items: 10
Threat Source Process Name	Time unit: Year	Sort by: Value (Descending)	Maximum items: 10
IPS Param Value	Time unit: Year	Sort by: Value (Descending)	Maximum items: 10

* When sorting groups by value(Asc/Desc), it's sorting groups by min/max values in the group.
* When sorting orders conflict with each other, the one of the parent group takes precedence.

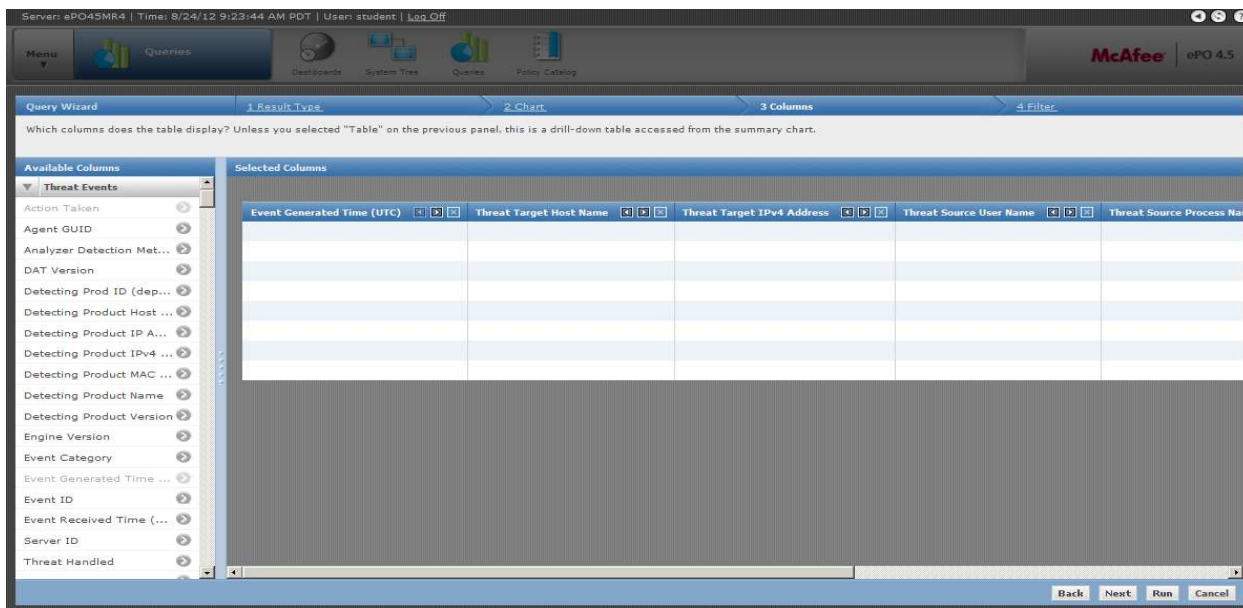
Back Next Run Cancel

If both HIPS 7 and HIPS 8 extensions are installed on the same EPO server, then there may be multiple fields with the same name, where each one will apply to only one HIPS version. It is essential to find the correct field that corresponds to the HOPS version you are using. Generally, the first field is for HIPS 7 and the second is for HIPS 8.

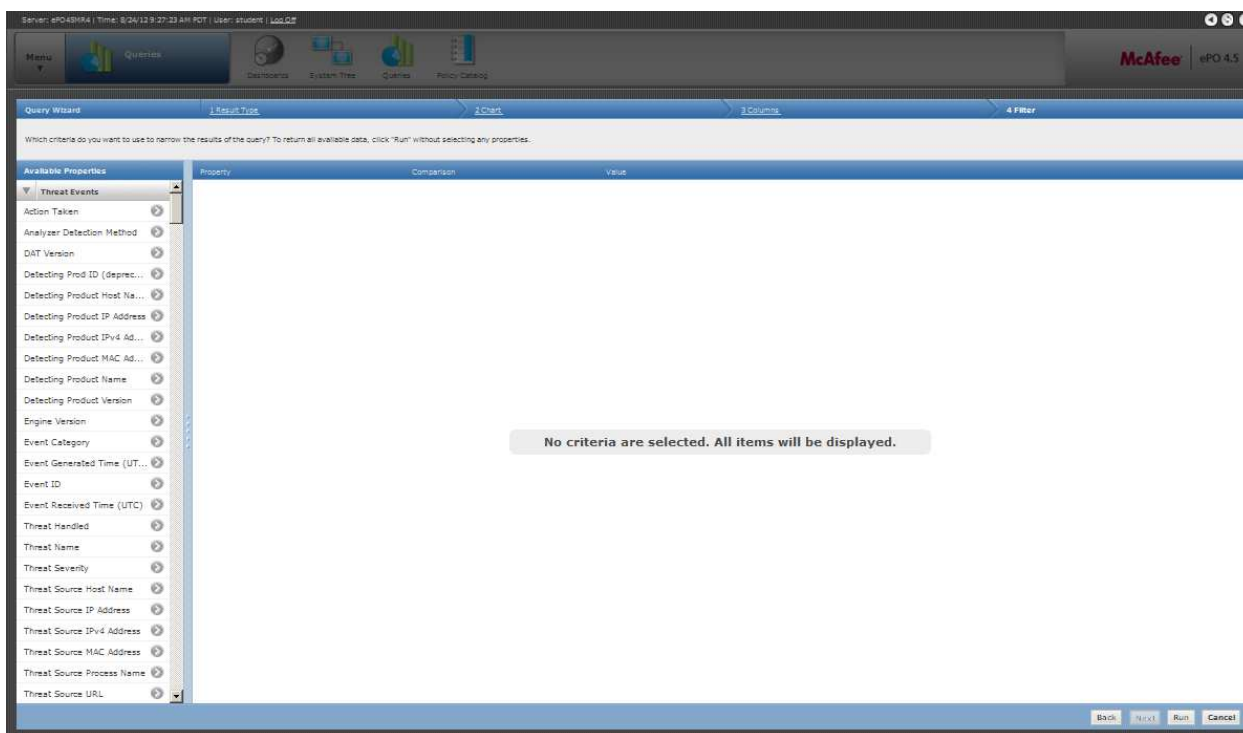
Select “Signature Name (Host IPS)” for the first “Labels are:” entry, click the “+” button to add another row, then select, “Threat Source Process Name”, add another row by clicking the “+”, then select “IPS Param Value” for the last row. Your screen should now look like the one above.

For the “3 Columns” Tab, add the following columns to the display:

Event Generated Time (UTC), Threat Target Host Name, Threat Target IPv4 Address, Threat Source User Name, Threat Source Process Name, IPS Param Value, Action Taken, Signature Name (Host IPS). Your screen will look similar to the one below. Click “Next” once you have completed this step.

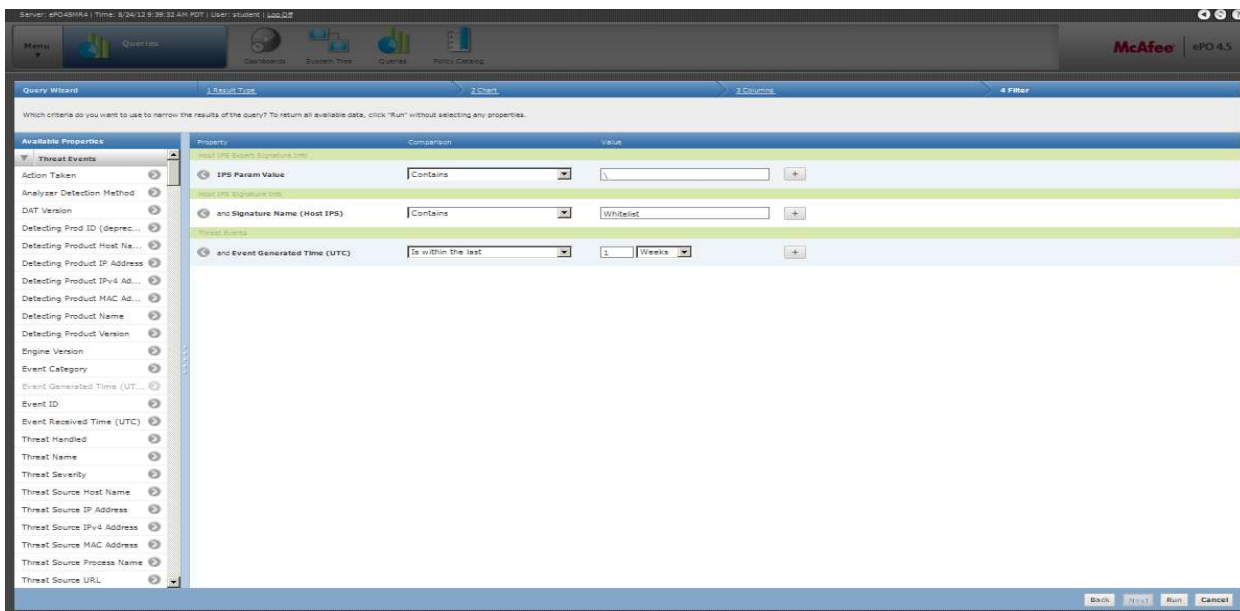


The next screen will appear as follows:



Add the following conditions to your filter by selecting the appropriate entry under “Available Properties”. Select the “IPS Param Name” property, change the “Comparison” to “Contains” and change the value to “files”. Next insert another “Available Property” named “Signature Name (Host IPS)” change the comparison to “Contains” and change the “Value” to “Whitelist”. Insert another “Available Property” named “Event Generate Time (UTC)”. Set the Comparison to “Is within the last” and set the Value to “1” “Week”. *You can change the value of the "Event Generated Time (UTC)" parameter to adjust the amount of time you will see the events for. As you tailor the policy over time, you will not need to see older events that have already been reviewed and addressed, so this will help filter out those older events.*

Your screen will now look as follows:



Now click the “Run” button to run your query. You will see Whitelisting events appear for the selected time period. The results will look similar to:

Application Whitelisting Execution Rule	Signature Name (Host IPS)	Number of Threat Events	Number of Threat Target Host Name
Application Whitelisting Execution Rule		29	14
C:\WINDOWS\EXPLORER.EXE		20	7
C:\Documents and Settings(Student.LOCAL\Desktop)\Poison Ivy 2.3.2.exe		7	1
C:\Documents and Settings(Student.LOCAL\Desktop)\calc.exe		4	1
C:\Documents and Settings(Student.LOCAL\Desktop)\calc1.exe		3	1
C:\temp\calc.exe		2	1
C:\WINDOWS\Temp\Poison Ivy 2.3.2.exe		2	1
C:\temp\08-07-2012 - ePO45MR4 FramePkg.exe		1	1
C:\temp\Poison Ivy 2.3.2.exe		1	1
C:\DOCUMENTS AND SETTINGS\STUDENT.LOCAL\DESKTOP\CALC.EXE		2	1
C:\Documents and Settings(Student.LOCAL\Desktop)\calc.exe		2	1
C:\DOCUMENTS AND SETTINGS\STUDENT.LOCAL\DESKTOP\POISON IVY 2.3.2.EXE		2	1
C:\Documents and Settings(Student.LOCAL\Desktop)\Poison Ivy 2.3.2.exe		2	1
Application Unknown		1	1
C:\Documents and Settings(Student.LOCAL\Desktop)\calc1.dll.exe		1	1
C:\PROGRAM FILES\VMWARE\VMWARE TOOLS\VMTOOLS.D.EXE		1	1
C:\Program Files\MSN\MSNCoreFiles\Unstall\mnmis.icc		1	1
C:\WINDOWS\SYSTEM32\DRWTSN32.EXE		1	1
C:\Documents and Settings(Student.LOCAL\Desktop)\Poison Ivy 2.3.2.exe		1	1
C:\WINDOWS\SYSTEM32\DWWIN.EXE		1	1
C:\Documents and Settings(Student.LOCAL\Desktop)\Poison Ivy 2.3.2.exe		1	1
C:\WINDOWS\SYSTEM32\RUNDLL32.EXE		1	1
C:\Documents and Settings(Student.LOCAL\Desktop)\calc1.dll		1	1
Application Whitelisting Modification Rule		6	5
C:\WINDOWS\EXPLORER.EXE		5	4
C:\WINDOWS\		2	1
C:\Program Files\calc1.exe		1	1
C:\Program Files\New Folder\		1	1

If you do not see any results, you may need to modify the database so that it will report events correctly. Follow the instructions in the section called [HIPS 8 workaround](#) on page 45.

Now Click “Save” to save your query so that you do not need to recreate it every time you need to see the Whitelisting events.

Server: ePO45MR4 | Time: 8/24/12 9:41:48 AM PDT | User: student | [Log Off](#)

Menu **Queries** Dashboards System Tree Queries Policy Catalog **McAfee** ePO 4.5

Save Query

Name:

Notes:

Groups:

☐ New group

☐ Private group (My Groups)

☐ Public group (Shared Groups)

☒ Existing groups

Make sure you name your policy and enter notes to describe your query. Also select the group where you want to save the query. Click on save to save the query to your ePO server. Now you can navigate to the group in the “Queries” tab and run the query directly as shown.

Server: ePO45MR4 | Time: 8/24/12 9:51:31 AM PDT | User: student | [Log Off](#)

Menu **Queries** Dashboards System Tree Queries Policy Catalog **McAfee** ePO 4.5

Groups

- All Queries
- My Groups
- Shared Groups
 - Data Loss Prevention
 - Enhanced Reporting
 - Findings
 - HOSTIPS_8000
 - Host IPS**
 - Mail Security - Domino
 - Mail Security - Exchange
 - McAfee Agent
 - Policy Assignment
 - Policy Auditor
 - Policy Auditor Rollup
 - Product Deployment
 - Rogue System Detection
 - SiteAdvisor Enterprise
 - System Management
 - TOPS Compliance
 - USAF ACCM Reports
 - User Auditing
 - VirusScan Enterprise

Queries

Quick find: ☐ Show selected rows

Queries	Actions
<input checked="" type="checkbox"/> Application Whitelisting Events This is a query for Application Whitelisting Events for a week.	Details Run Edit
<input type="checkbox"/> HIPS: App Block Create Status Displays where Application Blocking Creation is enabled on managed systems.	Details Run Edit
<input type="checkbox"/> HIPS: App Block Hook Status Displays where Application Blocking Hooking is enabled or disabled on managed systems.	Details Run Edit
<input type="checkbox"/> HIPS: Client Rules by Process HIP: Client Rules by Process	Details Run Edit
<input type="checkbox"/> HIPS: Client Rules by Process/Port Range HIP: Client Rules by Process/Port Range	Details Run Edit
<input type="checkbox"/> HIPS: Client Rules by Process/User HIP: Client Rules by Process/User	Details Run Edit
<input type="checkbox"/> HIPS: Client Rules by Protocol HIP: Client Rules by Protocol	Details Run Edit

Group Actions 1 selected

Clicking “Run” from this screen will run the selected query and return results without going through the “Edit” screens.

Signature Name (Host IPS) -> Threat Source Process Name -> IPS Param Value	Number of Threat Events	Number of Threat Target Host Name
Application Whitelisting Execution Rule	29	14
C:\WINDOWS\EXPLORER.EXE	20	7
C:\Documents and Settings\Student.LOCAL\Desktop\Poison Ivy 2.3.2.exe	7	1
C:\Documents and Settings\Student.LOCAL\Desktop\calc.exe	4	1
C:\Documents and Settings\Student.LOCAL\Desktop\calc1.exe	3	1
C:\temp\calc.exe	2	1
C:\WINDOWS\Temp\Poison Ivy 2.3.2.exe	2	1
C:\temp\08-07-2012 - ePO45MR4 FramePkg.exe	1	1
C:\temp\Poison Ivy 2.3.2.exe	1	1
C:\DOCUMENTS AND SETTINGS\STUDENT.LOCAL\DESKTOP\CALC.EXE	2	1
C:\Documents and Settings\Student.LOCAL\Desktop\calc.exe	2	1
C:\DOCUMENTS AND SETTINGS\STUDENT.LOCAL\DESKTOP\POISON IVY 2.3.2.EXE	2	1
C:\Documents and Settings\Student.LOCAL\Desktop\Poison Ivy 2.3.2.exe	2	1
Application Unknown	1	1
C:\Documents and Settings\Student.LOCAL\Desktop\calc1.dll.exe	1	1
C:\PROGRAM FILES\VMWARE\VMWARE TOOLS\VMTOOLS.DEXE	1	1
C:\Program Files\MSN\MSNCOREFILES\Install\msnms.ico	1	1
C:\WINDOWS\SYSTEM32\DRWTSN32.EXE	1	1
C:\Documents and Settings\Student.LOCAL\Desktop\Poison Ivy 2.3.2.exe	1	1
C:\WINDOWS\SYSTEM32\DWWIN.EXE	1	1
C:\Documents and Settings\Student.LOCAL\Desktop\Poison Ivy 2.3.2.exe	1	1
C:\WINDOWS\SYSTEM32\RUNDLL32.EXE	1	1
C:\Documents and Settings\Student.LOCAL\Desktop\calc1.dll	1	1
Application Whitelisting Modification Rule	6	5

Now, you have successfully built your Application Whitelisting Query. You can run this query to see what events are being generated by your Application Whitelisting policy.

HIPS 8 workaround

If you are running HIPS 8 and not HIPS 7, then you may not be able to get all of the information about threat events. Since the IPS Param Value field was introduced as part of the HIPS 7 Enhanced Reporting Extension and the HIPS 8 Enhanced Reporting Extension is not available yet, by default the IPS Param Value only reports events from HIPS 7. If you are only running HIPS 8 then this will show you a workaround to get HIPS to report the IPS Param Value. You will need access to the server that hosts the HBSS SQL database. ***Be sure to talk to an administrator of this database before making any changes. Make sure that this change to the database will not interfere with anything else on your network. You might have to get an administrator to do this for you.*** To do this work around you will need to edit a view in the HBSS database. The name of the view that you will need to edit is “dbo.ERP_View_HIP7_IPSEventParameter”. The default SQL for this view is:

```
SELECT EventID, ParameterName, ParameterValue
FROM dbo.HIP7_IPSEventParameter
```

You will need to change the HIP7_IPSEventParameter to HIP8_IPSEventParameter so that the view looks like the following:

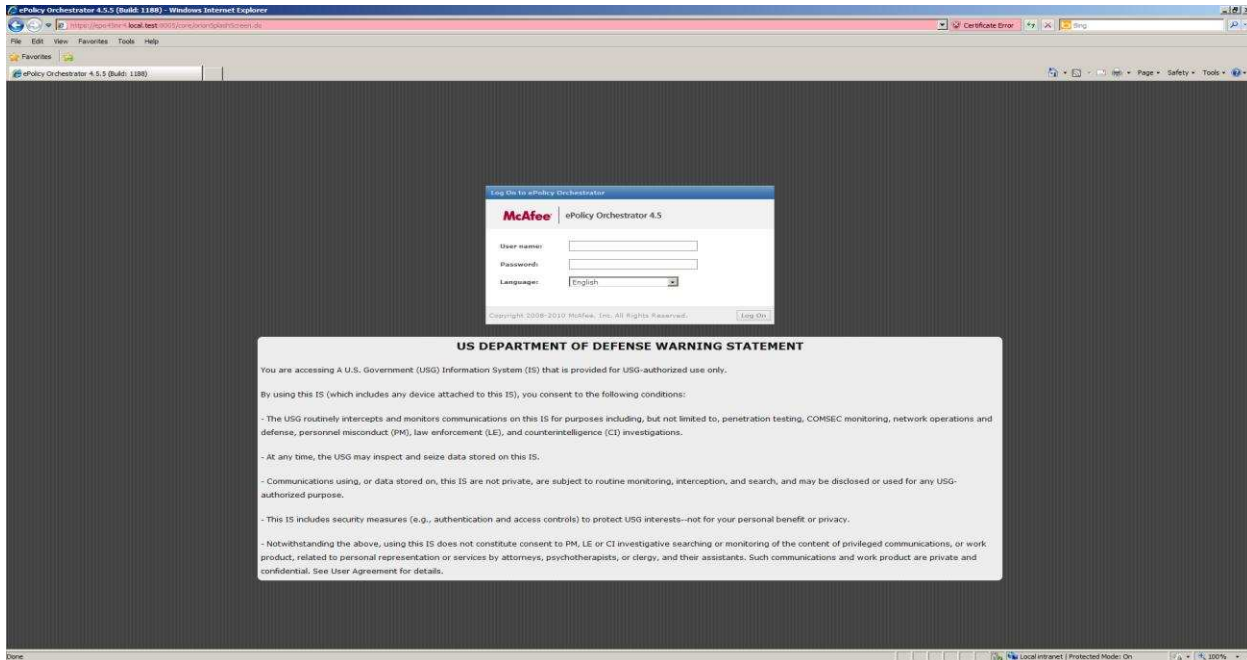
```
SELECT EventID, ParameterName, ParameterValue
FROM dbo.HIP8_IPSEventParameter
```

This will change the IPS Param Value field so that instead of reporting HIPS 7 information, the IPS Param Value field will now report HIPS 8 information.

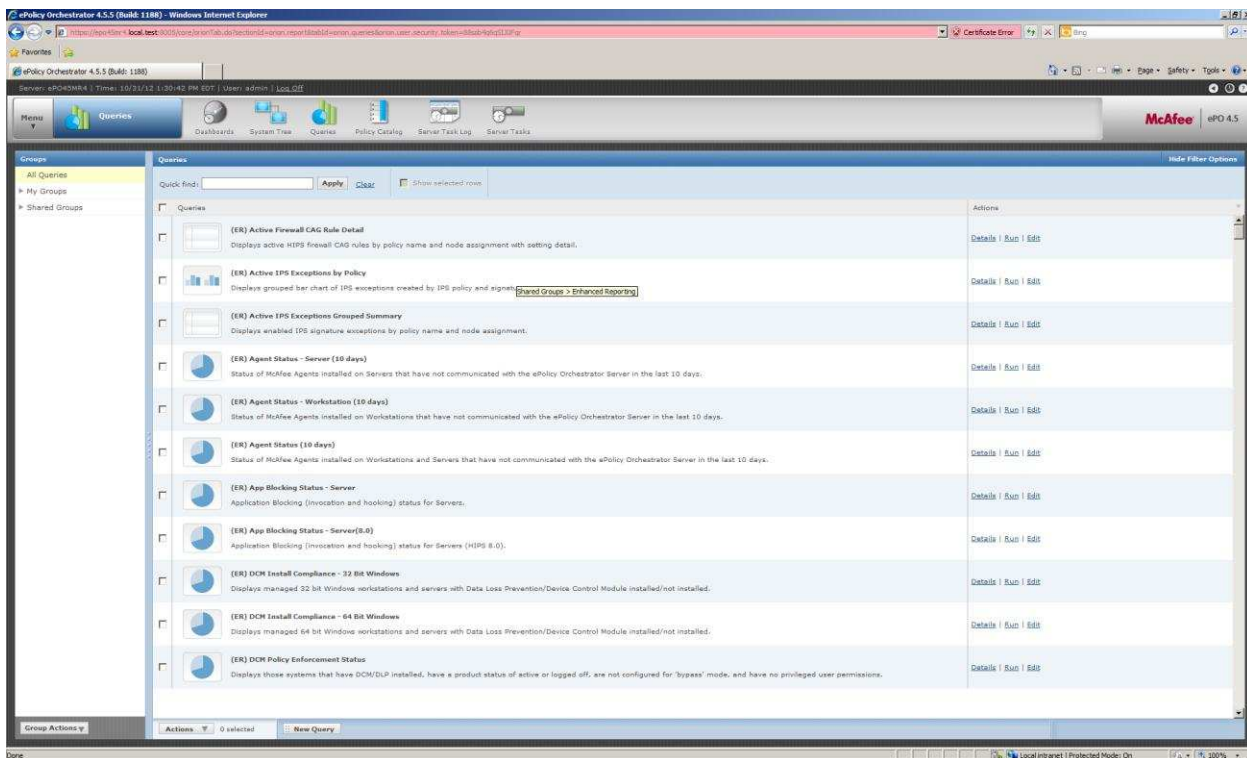
Reading query results

This section will show you how to identify important information from the results of the query that you just created in the section above.

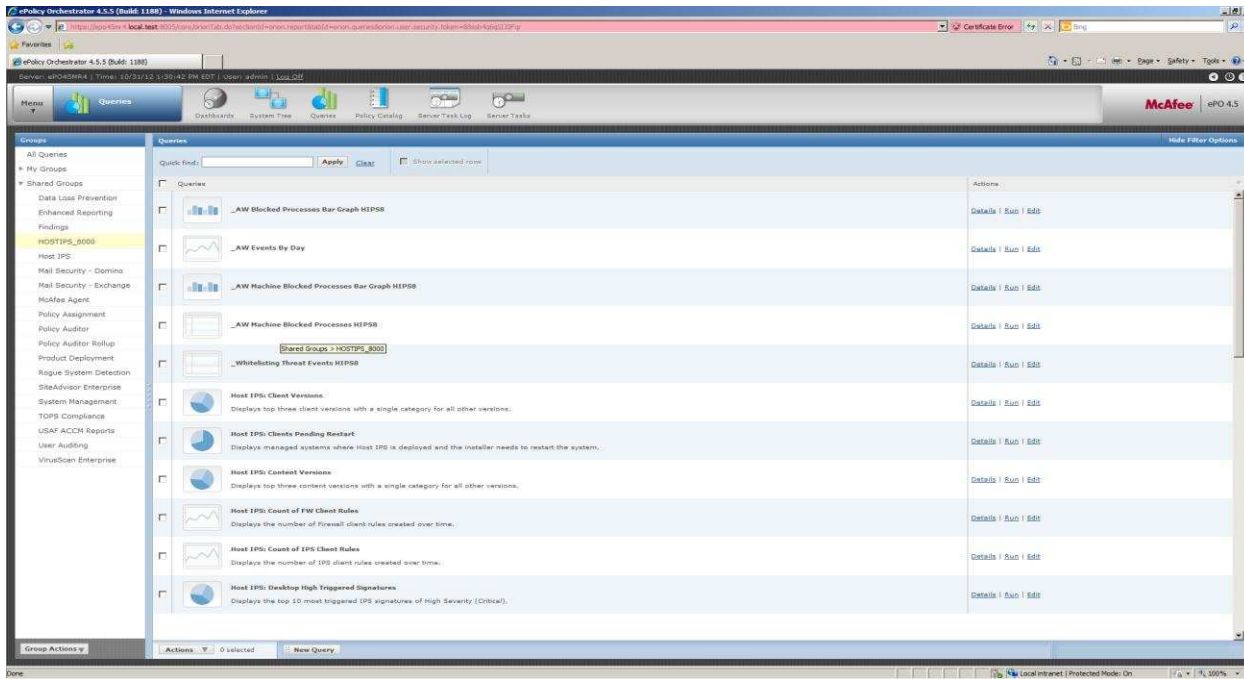
To run queries, first log on to the ePO server:



Click on the queries tab



Click on the category that contains your query



Click Run.

When you run the query that you created it will show a list of whitelisting events. There are several important pieces of information in this list. The important things in this list are the reason for blocking, name of the program that attempted execution, name of the file that was blocked from execution or modification, number of blocked attempts, and the number of machines where this event occurred.

Signature Name (Block IPS) - Threat Source Process Name - IPS Param Value	Number of Threat Events	Number of Threat Target Host Name
Application Whitelisting Execution Rule	Reason For Blocking	
C:\WINDOWS\EXPLORER.EXE	20	14
C:\Documents and Settings\Student.LOCAL\Desktop\Poison Ivy 2.3.2.exe	7	1
C:\Documents and Settings\Student.LOCAL\Desktop\calc.exe	4	1
C:\Documents and Settings\Student.LOCAL\Desktop\calc1.exe	3	
C:\temp\calc.exe	2	
C:\WINDOWS\Temp\Poison Ivy 2.3.2.exe	2	
C:\temp\08-07-2012 - ePO45MR4 FramePkg.exe	1	
C:\temp\Poison Ivy 2.3.2.exe	1	
C:\DOCUMENTS AND SETTINGS\STUDENT.LOCAL\DESKTOP\CALC.EXE	2	1
C:\Documents and Settings\Student.LOCAL\Desktop\calc.exe	2	1
C:\DOCUMENTS AND SETTINGS\STUDENT.LOCAL\DESKTOP\POISON IVY 2.3.2.EXE	2	1
C:\Documents and Settings\Student.LOCAL\Desktop\Poison Ivy 2.3.2.exe	2	1
Application Unknown	1	1
C:\Documents and Settings\Student.LOCAL\Desktop\calc1.dll.exe	1	1
C:\PROGRAM FILES\VMWARE\VMWARE TOOLS\VMTOOLS.DLL	1	1
C:\Program Files\MSN\MSNCoreFiles\Install\msnmsiico	1	1
C:\WINDOWS\SYSTEM32\DRWTSN32.EXE	1	1
C:\Documents and Settings\Student.LOCAL\Desktop\Poison Ivy 2.3.2.exe	1	1
C:\WINDOWS\SYSTEM32\DWWIN.EXE	1	1
C:\Documents and Settings\Student.LOCAL\Desktop\Poison Ivy 2.3.2.exe	1	1
C:\WINDOWS\SYSTEM32\WUNDLL32.EXE	1	1
C:\Documents and Settings\Student.LOCAL\Desktop\calc1.dll	1	1
Application Whitelisting Modification Rule	6	5

You can click on an entry in the list to get more information about that event. If you click on an entry that has more than one threat event another list will be generated that looks like the following picture. This list shows more individual information about specific threat events. It is important to note that Threat Source Process Name is the name of the file that was already running and attempted to execute or modify another file which is listed as the IPS Param value.

Advanced Filter ☐ Show selected rows

<input type="checkbox"/>	Event Generated Time (UTC)	Threat Target Host Name	Threat Target IPv4 Address	Threat Source User Name	Threat Source Process Name	IPS Param Value	Action Taken	Signature Name (Host IPS)
<input type="checkbox"/>	10/15/12 6:36:56 PM	WINXPCLIENT86	192.168.10.102	LOCAL\Student	C:\WINDOWS\EXPLORER.EXE	C:\Documents and Settings\Student\LOCAL\Desktop\NOTEPAD.EXE	Permitted	Application Whitelisting Execu
<input type="checkbox"/>	10/15/12 6:42:22 PM	WINXPCLIENT86	192.168.10.102	LOCAL\Student	C:\WINDOWS\EXPLORER.EXE	C:\Documents and Settings\Student\LOCAL\Desktop\NOTEPAD.EXE	Permitted	Application Whitelisting Execu
<input type="checkbox"/>	10/15/12 7:22:56 PM	WINXPCLIENT86	192.168.10.102	LOCAL\Student	C:\WINDOWS\EXPLORER.EXE	C:\WINDOWS\Resources\Themes\Luna\luna.msstyles	Permitted	Application Whitelisting Execu
<input type="checkbox"/>	10/15/12 8:08:37 PM	WINXPCLIENT86	192.168.10.102	LOCAL\Student	C:\WINDOWS\EXPLORER.EXE	C:\Documents and Settings\Student\LOCAL\Desktop\NOTEPAD.EXE	Blocked	Application Whitelisting Execu
<input type="checkbox"/>	10/15/12 8:37:33 PM	WINXPCLIENT86	192.168.10.102	LOCAL\Student	C:\WINDOWS\EXPLORER.EXE	C:\Documents and Settings\Student\LOCAL\Desktop\NOTEPAD.EXE	Permitted	Application Whitelisting Execu
<input type="checkbox"/>	10/17/12 2:47:41 PM	WINXPCLIENT86	192.168.10.102	LOCAL\Student	C:\WINDOWS\EXPLORER.EXE	C:\Documents and Settings\Student\LOCAL\Desktop\NOTEPAD.EXE	Permitted	Application Whitelisting Execu
<input type="checkbox"/>	10/17/12 2:48:48 PM	WINXPCLIENT86	192.168.10.102	LOCAL\Student	C:\WINDOWS\EXPLORER.EXE	C:\Documents and Settings\Student\LOCAL\Desktop\NOTEPAD.EXE	Permitted	Application Whitelisting Execu
<input type="checkbox"/>	10/17/12 3:07:08 PM	WINXPCLIENT86	192.168.10.102	LOCAL\Student	C:\WINDOWS\EXPLORER.EXE	C:\Documents and Settings\Student\LOCAL\Desktop\NOTEPAD.EXE	Permitted	Application Whitelisting Execu
<input type="checkbox"/>	10/17/12 7:43:05 PM	WINXPCLIENT86	192.168.10.102	LOCAL\Student	C:\WINDOWS\EXPLORER.EXE	C:\Documents and Settings\Student\LOCAL\Desktop\NOTEPAD.EXE	Permitted	Application Whitelisting Execu
<input type="checkbox"/>	10/18/12 6:45:39 PM	WINXPCLIENT86	192.168.10.102	LOCAL\Student	C:\WINDOWS\EXPLORER.EXE	C:\WINDOWS\Resources\Themes\Luna\luna.msstyles	Permitted	Application Whitelisting Execu
<input type="checkbox"/>	10/18/12 6:46:58 PM	WINXPCLIENT86	192.168.10.102	LOCAL\Student	C:\WINDOWS\EXPLORER.EXE	C:\Documents and Settings\Student\LOCAL\Desktop\poisonivy.EXE	Permitted	Application Whitelisting Execu

Actions 0 selected Show Source Systems Show Target Systems Back Close

If you click on an event in the list above, or if you clicked on an entry in the original list that only had one threat event then you will see a detailed view of the threat event. This detailed view lists all information that HBSS has stored on that threat event. The important things are circled in red.

Threat Event Log Details	
Threat Event Log Information	
Server ID:	eP045MR4
Event Received Time (UTC):	10/18/12 4:45:25 PM
Event Generated Time (UTC):	10/18/12 4:47:28 PM
Agent GUID:	27550B5F-893C-4779-8CF2-2A0D703DFC7
Detecting Prod ID (deprecated):	HOSTIPS_8000
Detecting Product Name:	McAfee Host Intrusion Prevention
Detecting Product Version:	8.0.0
Detecting Product Host Name:	WINXPCLIENT86
Detecting Product IPv4 Address:	192.168.10.102
Detecting Product IP Address:	0:0:0:0:0:0:ffff:0a8:a66
Detecting Product MAC Address:	000c292bf106
DAT Version:	
Engine Version:	
Threat Source Host Name:	
Threat Source IPv4 Address:	192.168.10.102
Threat Source IP Address:	0:0:0:0:0:0:ffff:0a8:a66
Threat Source MAC Address:	
Threat Source User Name:	LOCAL\Student
Threat Source Process Name:	C:\DOCUMENTS AND SETTINGS\STUDENT\LOCAL\DESKTOP\POISONVYVY.EXE
Threat Source URL:	file:///C:/DOCUMENTS AND SETTINGS/STUDENT/LOCAL/DESKTOP/POISONVYVY.EXE
Threat Target Host Name:	WINXPCLIENT86
Threat Target IPv4 Address:	192.168.10.102
Threat Target IP Address:	0:0:0:0:0:0:ffff:0a8:a66
Threat Target MAC Address:	000c292bf106
Threat Target User Name:	
Threat Target Port Number:	
Threat Target Network Protocol:	
Threat Target Process Name:	
Threat Target File Path:	
Event Category:	File system
Event ID:	18000
Threat Severity:	Information
Threat Name:	4001
Threat Type:	Execute
Action Taken:	Permitted
Threat Handled:	false
Analyzer Detection Method:	
Threat Event Descriptions	
Event Description:	Host intrusion detected and handled
Host IPS 8.0 Event Information	
View Host IPS Event Description	
Drive Type	HardDrive
ePO Reachable	Unknown
Executable file description	NOTEPAD
Executable fingerprint	5e28284f9b5f9097640d59a73d38ad4c
Files	C:\Documents and Settings\Student\LOCAL\Desktop\poisonivy.EXE
In Trusted Network	Unknown
Subject Distinguished Name	CN=MICROSOFT WINDOWS COMPONENT PUBLISHER, O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US
Subject Organization Name	MICROSOFT CORPORATION
Workstation Name	WINXPCLIENT86
Host IPS Event Information	
This is not an IPS event.	
Related Items	
Go to related System	

Tailoring

In this section you will create application whitelisting exceptions. The exceptions that you create will be based on reviewing the logs to see if any applications need exceptions to run. Every time you tailor the policy be sure to save it, export it from the utility, and import it into the ePO server to apply the new policy.

You should wait until you have several days of logs generated by the test policy before you attempt this step. In order to create effective exceptions, your logs need to have enough data to reflect normal system usage.

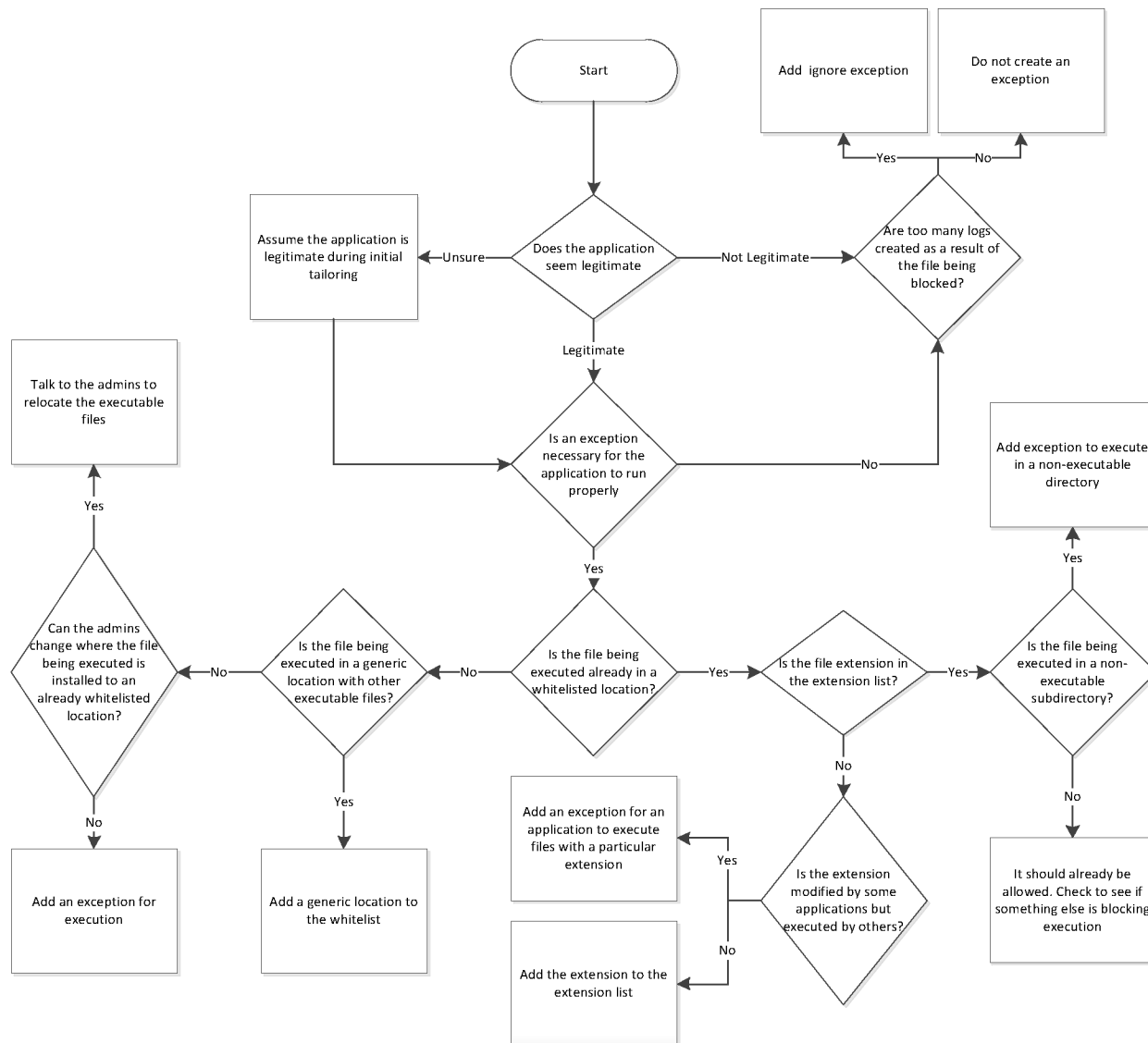
During initial tailoring, assume for ease of implementation that application behaviors are legitimate. Later, during enforcement, assume opposite.

Decision Tree for Execution

The following decision tree will help you decide if you need to create an exception for an application to run. The decision tree is listed in two forms below: the graphic and a text based version. Both versions show the same process that you take to decide if you should create an exception and what kind of exception you should create. Included in the process are links to specific instructions in this document that show you how to create specific exceptions.

It is important when creating exceptions to make them neither too general nor too specific. If exceptions allow more flexibility than is needed, it could lead to Application Whitelisting being ineffective and easily circumvented. If exceptions are too specific, then many files may need to be part of an exception, and if there are any slight changes to the app, the exception may no longer properly apply. The exception may no longer properly apply.

Visual decision tree



Click on a link below to go to instructions in this document on how to create a specific exception.

[Add a generic location to the whitelist](#), page 60

[Add an exception for application execution](#), page 58

[Add the extension to the executable extension list](#), page 58

[Add exception to execute in a non-executable directory](#), page 58

[Check to see if something else is blocking execution](#), page 61

[Add ignore exception](#), page 55

[Add an exception for an application to execute files with a particular extension](#), page 58

Text version of the decision tree

Start with step 1 and answer the questions to determine what to do with an application that may need an exception.

1. Does the application seem legitimate and does it have normal application behavior?
 - 1.1. If you are unsure then assume that the application is legitimate during initial tailoring.
2. If the application is illegitimate then do not change the policy because the application should be blocked.
 - 2.1. If the application is blocked too often and creates too many events, then add an ignore exception so that it will not be logged. [Add ignore exception](#), page 55
3. If the application is legitimate, would blocking the behavior cause an issue with the application? In other words, is an exception necessary for the application to run properly?
 - 3.1. If yes, continue to step 4.
 - 3.2. If no, then do not create new exception
 - 3.2.1. If the application behavior is blocked too often and creates too many log events, then add an ignore exception so that it will not be logged. [Add ignore exception](#), page 55
4. If the application needs to be allowed to execute, is the file being executed already in a whitelisted location?
 - 4.1. If yes, then is the file extension already in the file extension list?
 - 4.1.1. If no, is the extension likely used with files that are modified by some programs but this particular program needs to execute files with this extension? (Example: .dat files are modified by some programs but could be executed by some other programs.)
 - 4.1.1.1. If yes, then add an exception for that program to execute files with that extension. [Add an exception for an application to execute files with a particular extension](#), page 58
 - 4.1.1.2. If no, add the file extension to the whitelisted executable extension list. [Add the extension to the whitelisted executable extension list](#), page 58
 - 4.1.2. If yes, is the file being executed in a non-executable subdirectory of a whitelisted directory?
 - 4.1.2.1. If yes, then add an exception for that file to be executed in a non-executable subdirectory. [Add exception to execute in a non-executable directory](#), page 58
 - 4.1.2.2. If no, then it should already be allowed. See if something else is blocking the application or if there is an ignore exception that is blocking execution. [Check to see if something else is blocking execution](#), page 61
 - 4.2. If no, is the file being executed in a generic location with other executable files?
 - 4.2.1. If yes, then add a generic location to the whitelist. [Add a generic location to the whitelist](#), page 60

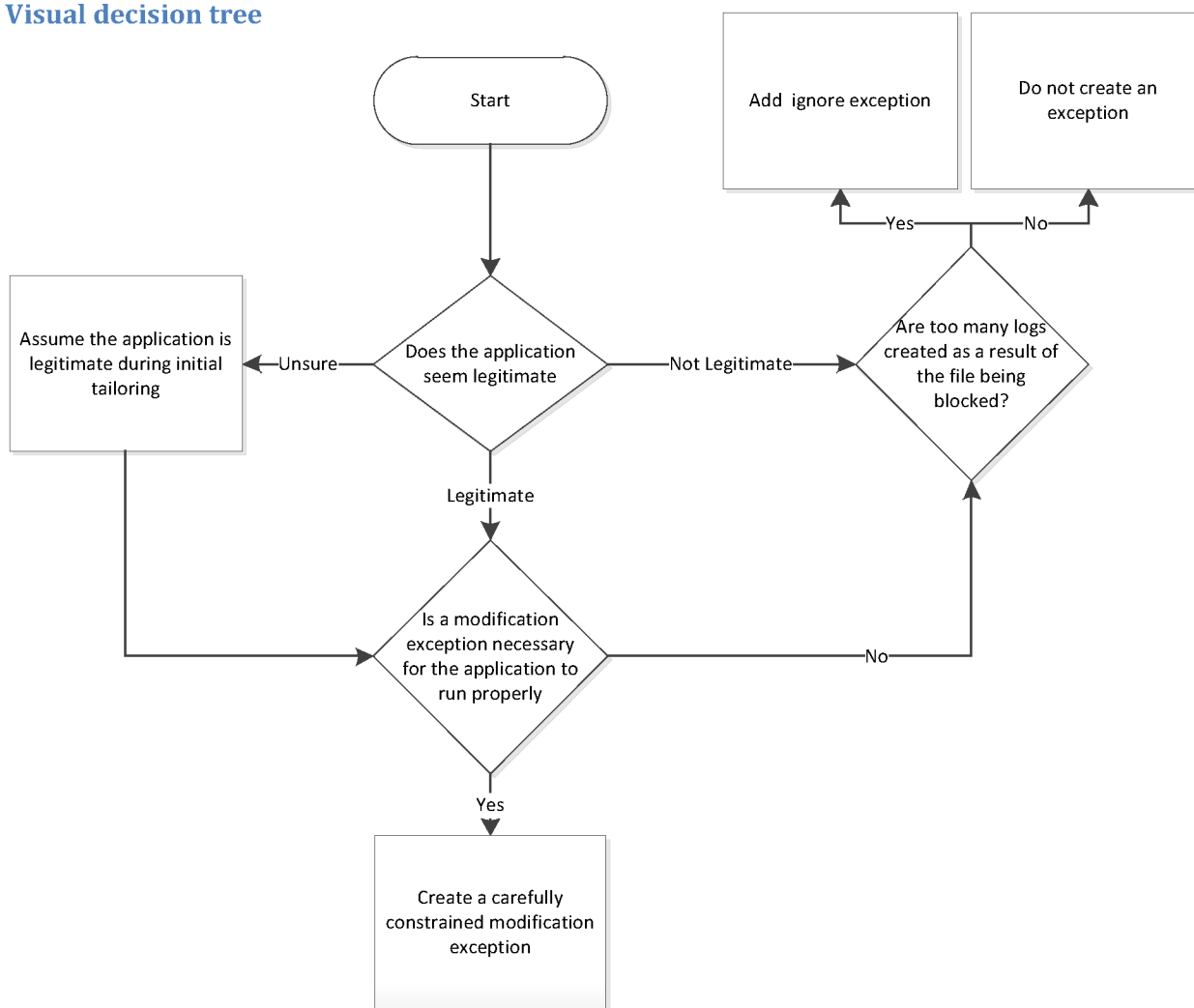
- 4.2.2. If no, can the admins change where the file being executed is installed to an already whitelisted location?
- 4.2.2.1. If yes, then talk to the admins to relocate the executable files.
 - 4.2.2.2. If no, then add an exception for execution but be sure to carefully constrain the exception and make it generic enough for all similar files that the application will be executing. [Add an exception for application execution](#), page 58

Decision tree for modification

This decision tree will help you decide if you need to create a modification rule exception. The HIPS application rules only block modification to executable files. In most cases a modification exception is not needed, many programs will request modification privileges on an executable but never actually modify that executable. The important thing to remember when creating modification rules is that if the program runs without a modification exception, then it does not need one. Included with the decision tree are links to specific instructions in this document that show you how to create specific exceptions.

It is important when creating exceptions not to make the too general. If exceptions allow more flexibility than is needed it could lead to Application Whitelisting being ineffective and easily circumvented. If exceptions are too specific, then many files may need to be part of an exception, and if there are any slight changes to the app, the exception may no longer properly apply.

Visual decision tree



Click on a link below to go to instructions in this document on how to create a specific exception.

[Add ignore exception](#), page 55

[Add a carefully constrained modification rule](#), page 64

Text version of a decision tree

Start with step 1 and answer the questions to determine what to do with an application that may need an exception.

1. Does the application seem legitimate and does it have normal application behavior?
 - 1.1. If you are unsure then assume that the application is legitimate during initial tailoring.
2. If the application is illegitimate then do not change the policy because the application should be blocked.
 - 2.1. If the application is blocked too often and creates too many log events, then add an ignore exception so that it will not be logged. [Add ignore exception](#), page 55
3. If the application is legitimate, is a modification exception necessary for the application to run properly?
 - 3.1. If yes, continue to step 4.
 - 3.2. If no, then do not create new exception
 - 3.2.1. If the application is blocked too often and creates too many logs, then add ignore exception so that it will not be logged. [Add ignore exception](#), page 55
4. Create a carefully constrained modification rule that only allows specific files to be modified. [Add a carefully constrained modification rule](#), page 64

Specific Instructions

All instructions assume that you are using the HIPS application whitelisting tool to configure the application whitelisting policy.

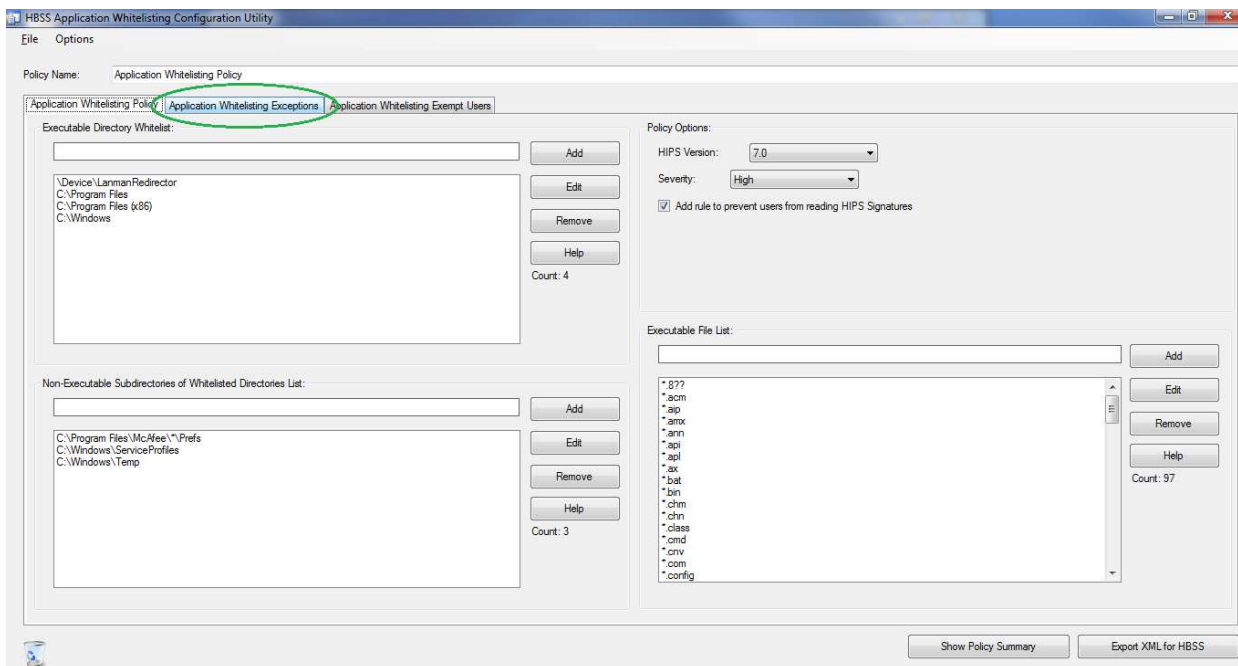
When creating exceptions, be careful not to allow too much flexibility within temporary directories or giving more flexibility than is needed to applications.

Use the same policy name when updating an existing policy to be assigned to the same computers. Use a different policy name for a new policy to apply to different computers.

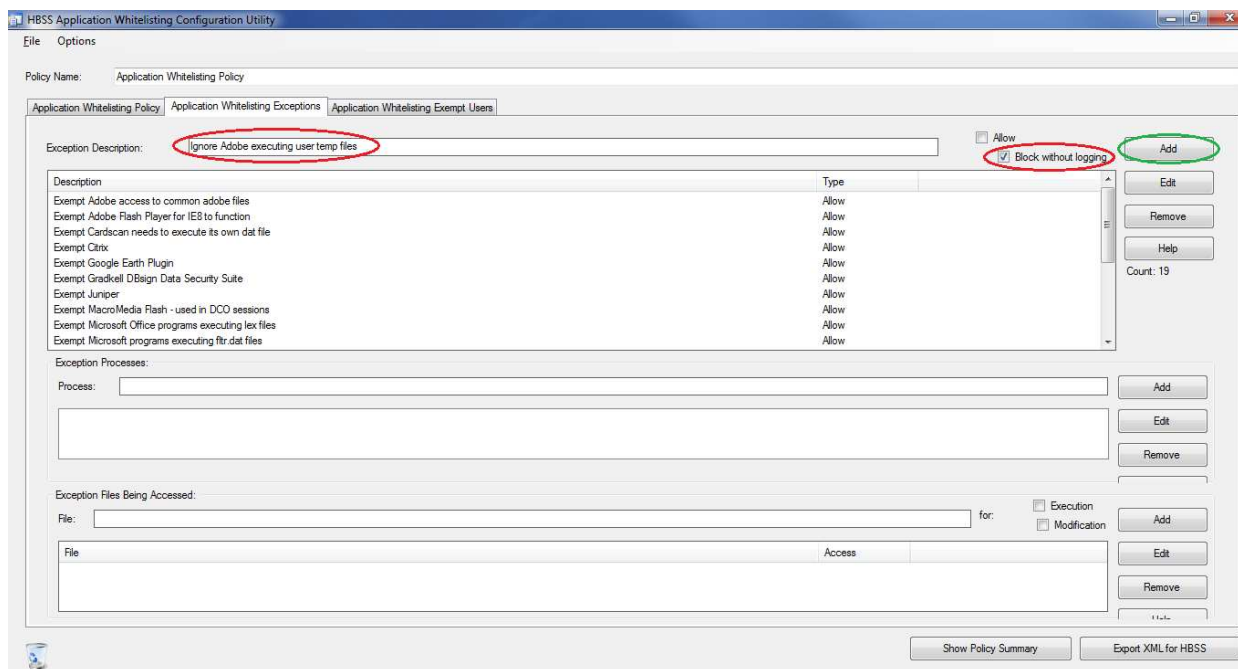
How to Add an Ignore Exception

Open the HBSS application whitelisting configuration utility.

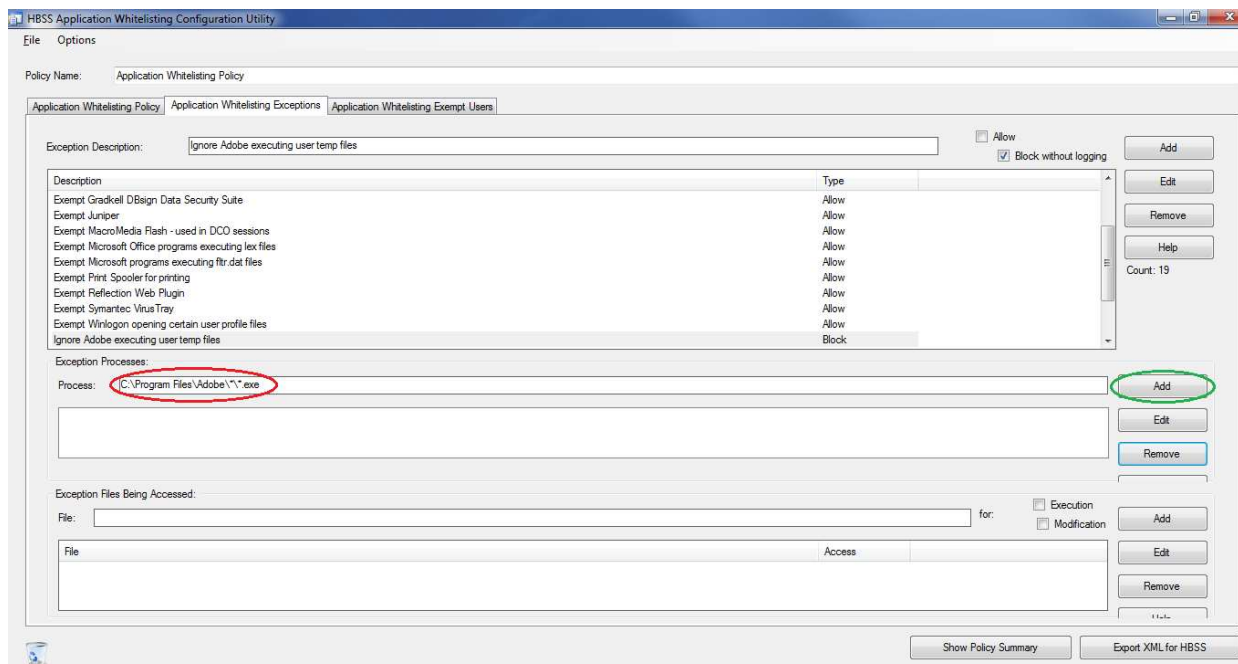
Click on the **Application Whitelisting Exceptions** tab



Next, type in a name for the **Exception Description**, check the **Block Without Logging** box, then click **Add**. If there is an existing exception that is similar to the new exception you are adding, consider adding to the existing exception instead of creating a new exception.

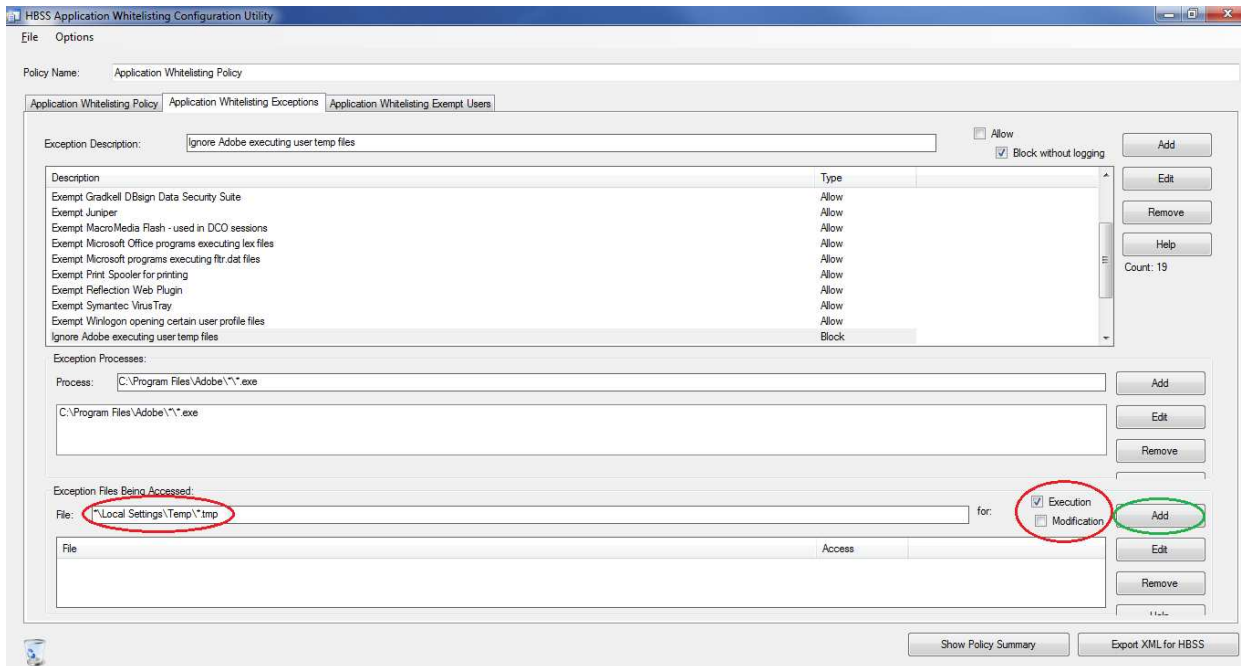


The exception description you just created will now be highlighted in the list. Type in the **Exception Process** (Note: This is not the application that will be blocked without logging; this is the program that is already running that attempts to execute or modify the program that will be blocked without logging). If you want block without logging globally, type in “?:*”. After you have typed the **Exception Process**, click **Add**. (Note: This can be done for more than one application process as part of a single exception.)



Next, type in the **Exception Files Being Accessed** (This is the file that you want to block without logging or the file that is being modified), check the **Execution** box or the **Modification** box depending on what you are blocking, then press **Add**. (Note: This can be done for more than one file as part of a single exception.)

Tip: Use `*\NameOfProcess.exe` to apply regardless of where the application is installed or `?:\PathToApplication*.exe` for all files associated with a particular application.



Be sure to save any changes that you make to your policy.

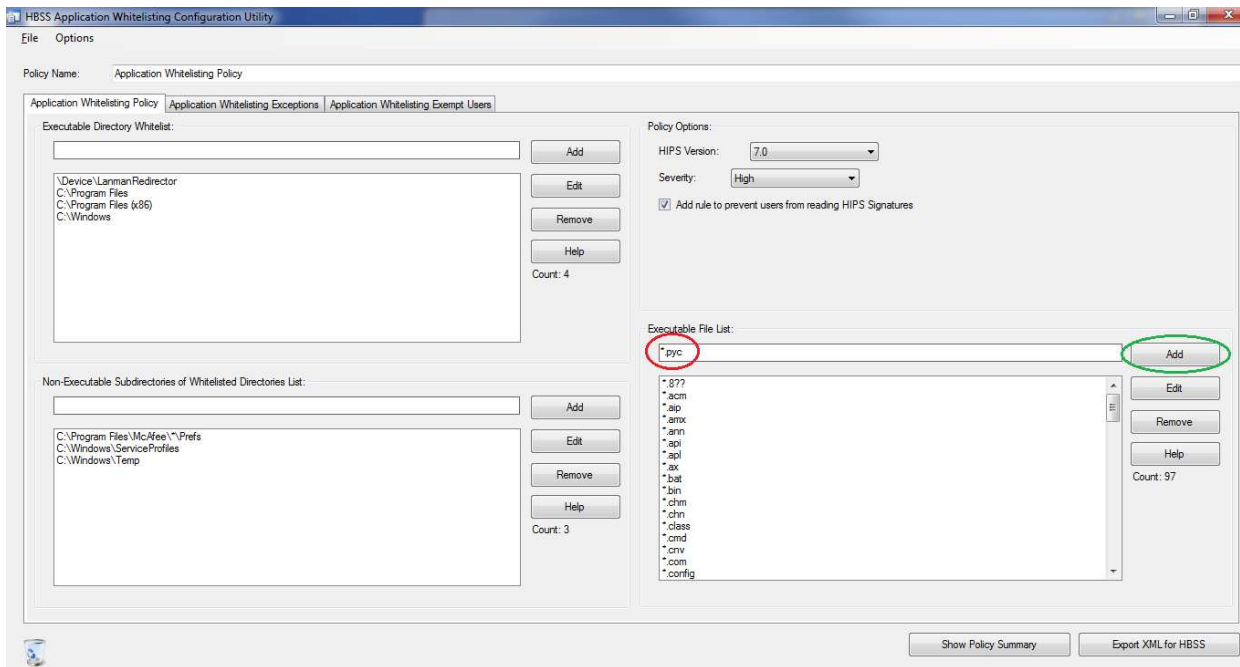
Note: In the case of execution the **exception process** is the program that will try to execute the exception files being accessed. An example of this is when you run notepad from the start menu, explorer.exe is the program that attempts to execute notepad.exe. If the **exception process** was set as explorer.exe and you tried to double click on notepad to execute it and it was set as the **exception files being accessed**. then notepad's execution would be blocked without logging. If you tried to execute notepad from the command prompt (cmd.exe) and cmd.exe was not set as an **exception process** then a log would be generated even if notepad is set in **exception files being accessed**.

In the case of modification the **exception process** is the program that is trying to modify another file. The **exception files being accessed** is the file that is being modified.

Add a Whitelisted Executable Extension

Open the HBSS application whitelisting configuration utility.

To add an executable extension, type the extension into the **Executable File List** box and press **Add**. Be sure to include **“*.”** before the extension. (Example: To add compiled python files use **“*.pyc”**)

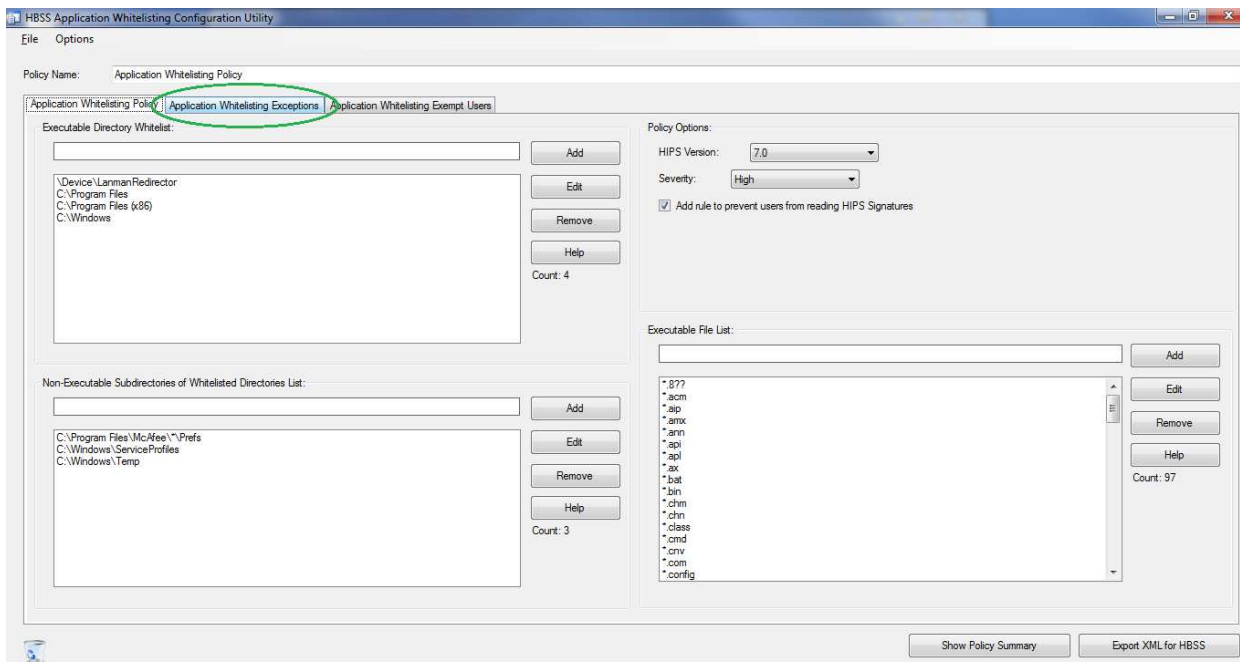


Be sure to save any changes that you make to your policy.

Add a Carefully Constrained Execution Exception

Open the HBSS application whitelisting configuration utility.

To add an execution exception, click on the **application whitelisting exceptions** tab.



Type in a name for the exception in the **Exception Description** box, check the **Allow** box, and then press **Add**. If there is an existing exception that is similar to the new exception you are adding, consider adding to the existing exception instead of creating a new exception.

Policy Name: Application Whitelisting Policy

Application Whitelisting Policy | Application Whitelisting Exceptions | Application Whitelisting Exempt Users

Exception Description: Allow Putty to Run on the Desktop ☒ Allow ☐ Block without logging **Add**

Description

Description	Type
Allow Open Cobol to execute .dat files	Allow
Exempt Adobe access to common adobe files	Allow
Exempt Adobe Flash Player for IES to function	Allow
Exempt Cardscan needs to execute its own dat file	Allow
Exempt Citrix	Allow
Exempt Google Earth Plugin	Allow
Exempt Gradell DBaig Data Security Suite	Allow
Exempt Juniper	Allow
Exempt MacroMedia Flash - used in DCO sessions	Allow
Exempt Microsoft Office programs executing lex files	Allow

Exception Processes:

Process: **Add**

Edit

Remove

Exception Files Being Accessed:

File: for: ☐ Execution ☐ Modification **Add**

Edit

Remove

Show Policy Summary Export XML for HBSS

Type in the **Exception Processes**, this is the program that is trying to execute another program or library (Example: When you run notepad from the start menu, explorer.exe attempts to run notepad.exe, so explorer.exe would be the exception process). Click the **Add** button. (Note: This can be done for more than one program as part of a single exception).

Policy Name: Application Whitelisting Policy

Application Whitelisting Policy | Application Whitelisting Exceptions | Application Whitelisting Exempt Users

Exception Description: Allow Putty to Run on the Desktop ☒ Allow ☐ Block without logging **Add**

Description

Description	Type
Allow Open Cobol to execute .dat files	Allow
<u>Allow Putty to Run on the Desktop</u>	Allow
Exempt Adobe access to common adobe files	Allow
Exempt Adobe Flash Player for IES to function	Allow
Exempt Cardscan needs to execute its own dat file	Allow
Exempt Citrix	Allow
Exempt Google Earth Plugin	Allow
Exempt Gradell DBaig Data Security Suite	Allow
Exempt Juniper	Allow
Exempt MacroMedia Flash - used in DCO sessions	Allow

Exception Processes:

Process: explorer.exe **Add**

Edit

Remove

Exception Files Being Accessed:

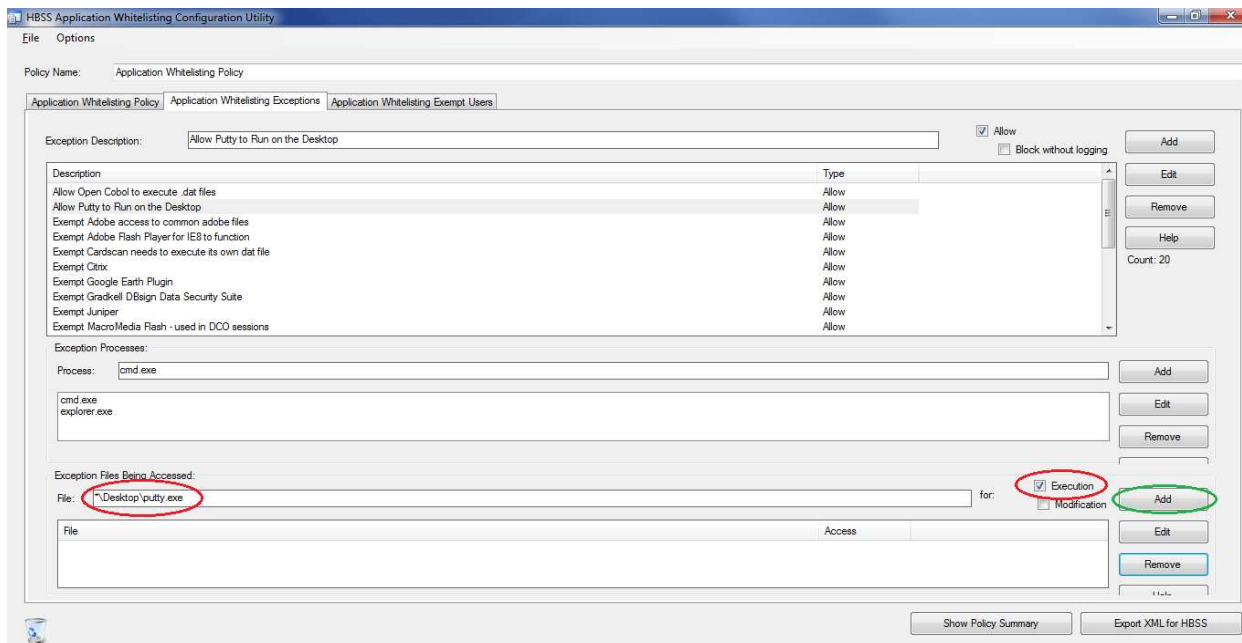
File: for: ☐ Execution ☐ Modification **Add**

Edit

Remove

Show Policy Summary Export XML for HBSS

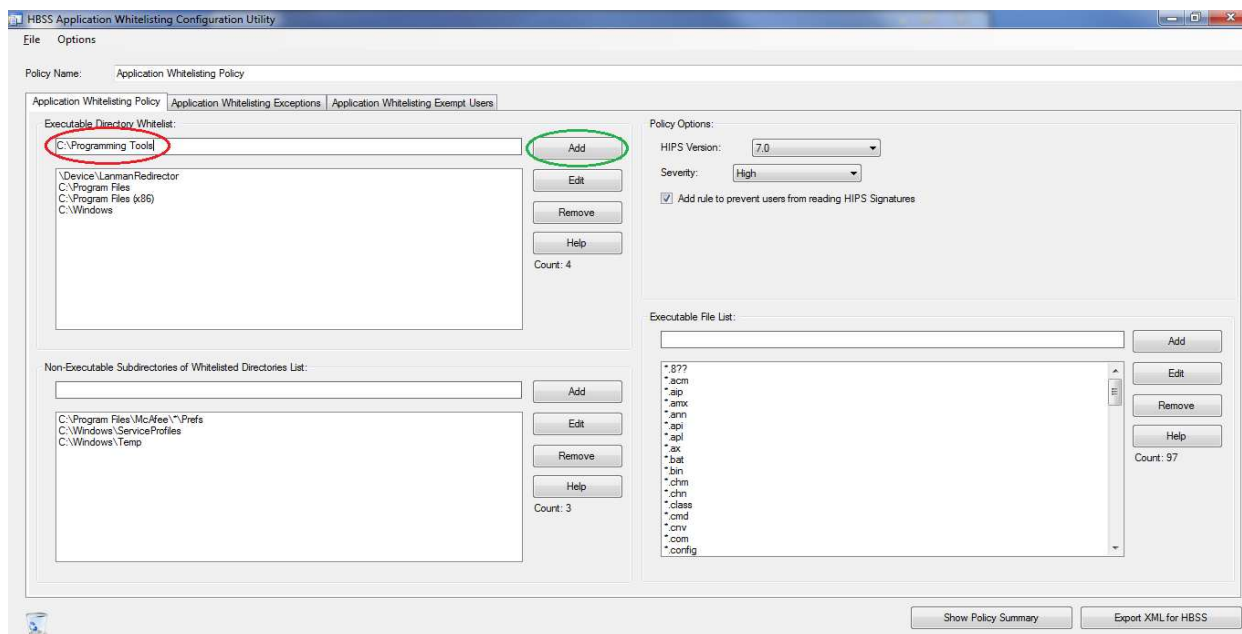
Type in the **Exception Files Being Accessed**, this identifies the files that will be executed (Example: When you run notepad from the start menu, explorer.exe attempts to run notepad.exe, so notepad.exe would be the exception file being accessed). Check the **Execution** box, then click the **Add** button. (Note: This can be done for more than one program).



Be sure to save any changes that you make to your policy.

Add a Generic Location to the Whitelist

To add a generic location to the whitelist, type in the path for the whitelist into the **Executable Directory Whitelist** box, then click **Add**.

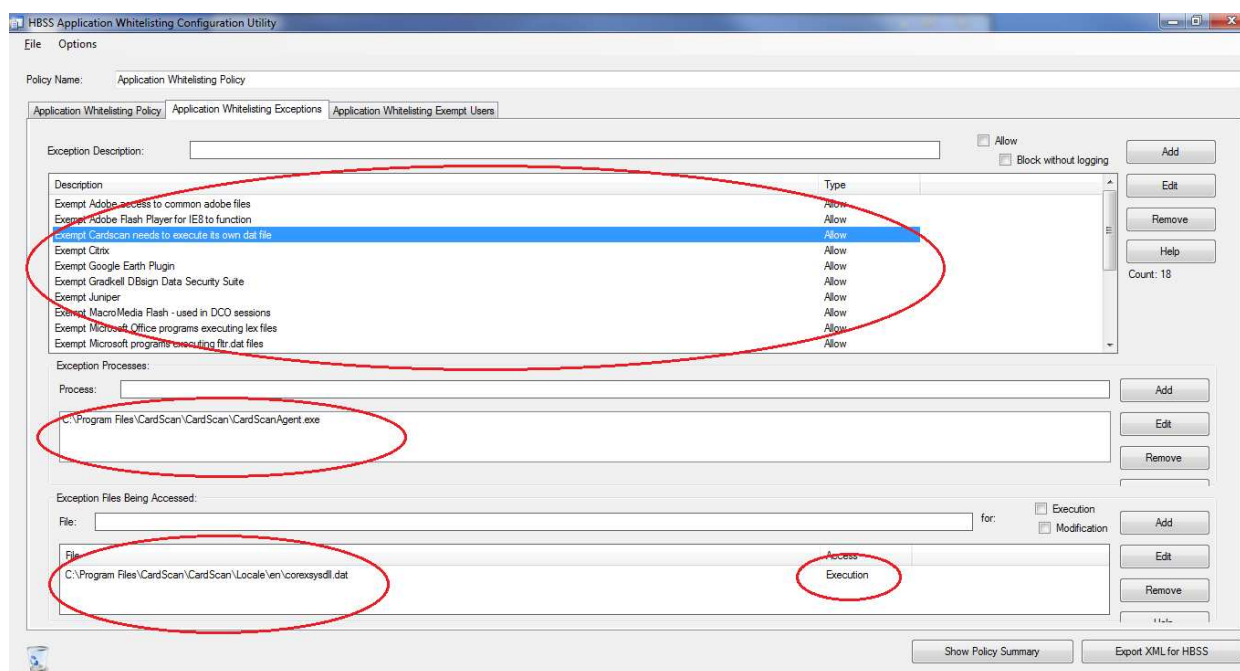


Be sure to save any changes that you make to your policy.

It is important to realize that all executable files within whitelisted directories will now be allowed to execute, but they will also now be protected from modifications.

Check to see if an exception is blocking execution

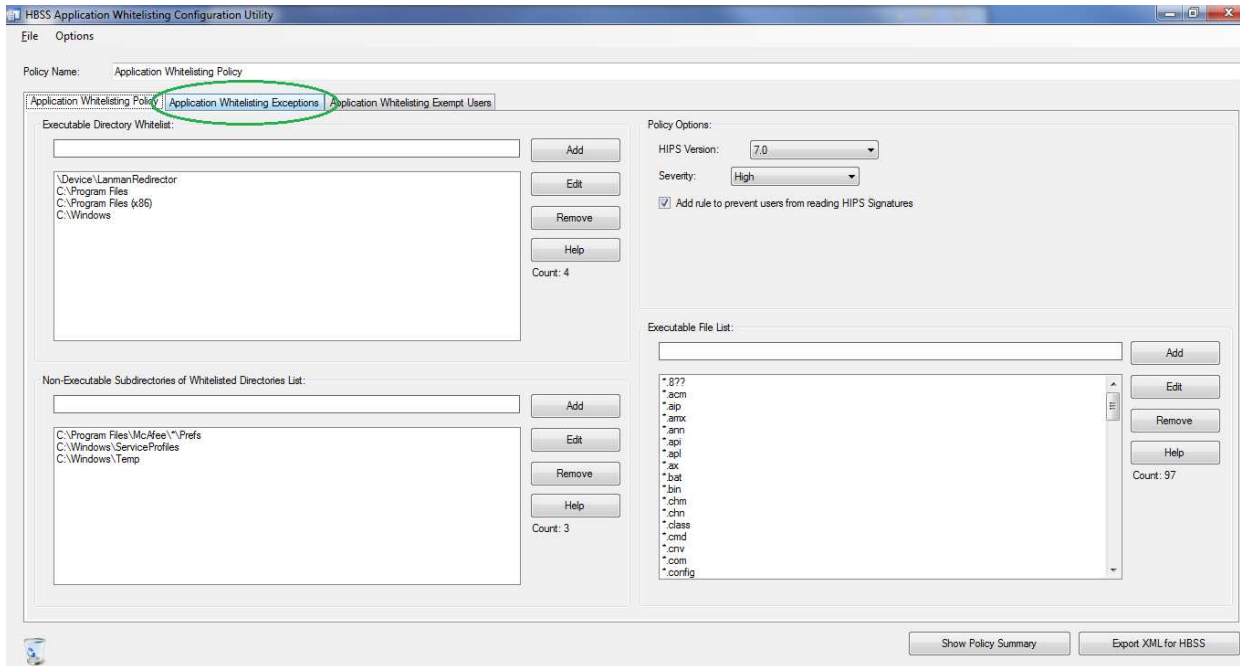
If there are no application whitelisting events being reported but an application is not working correctly and receiving access denied errors for execution or modification for executable files, a block without logging exception could be the case. To see if this is the case in the **Application Whitelisting Exceptions** tab in the application whitelisting configuration utility, check all exceptions whose type is “blocked”. This will appear in the event description area. For all “blocked” rules, check the **Exception Process** and the **Exception Files Being Accessed** to see if your program is in the list. If you cannot find your program in the **Application Whitelisting Exceptions**, check with your administrator to see if there are any other policies that may be blocking execution of the program.



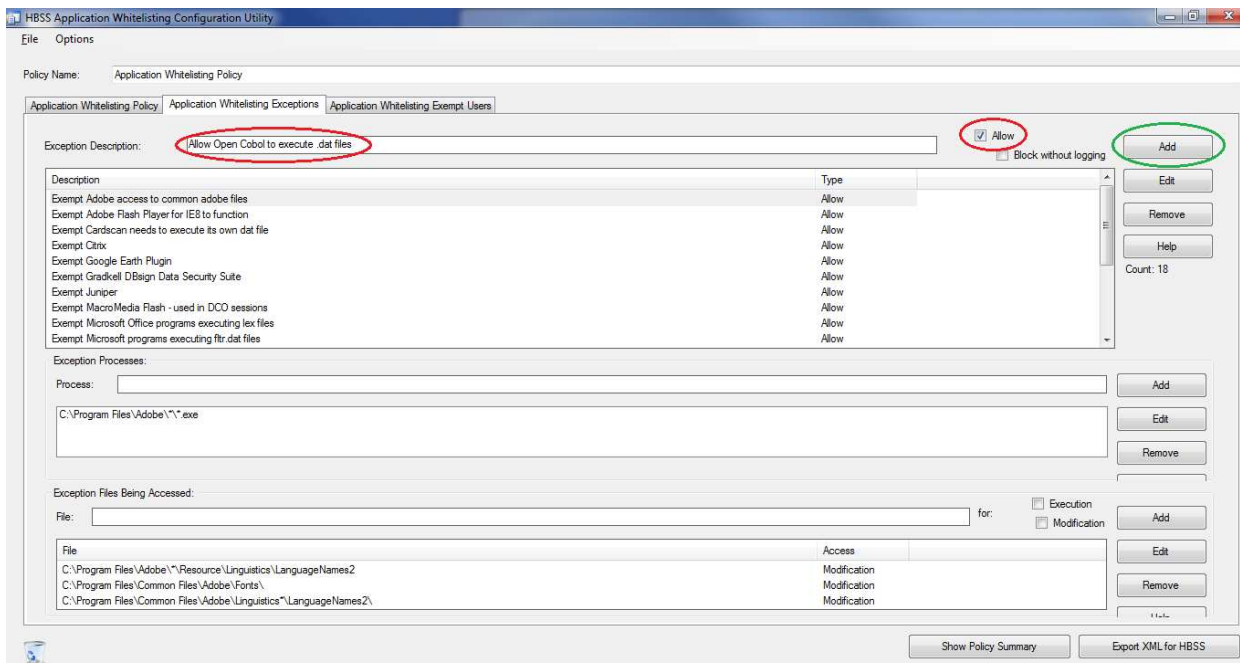
Add an exception for an application to execute files with a particular extension

Open the HBSS application whitelisting configuration utility.

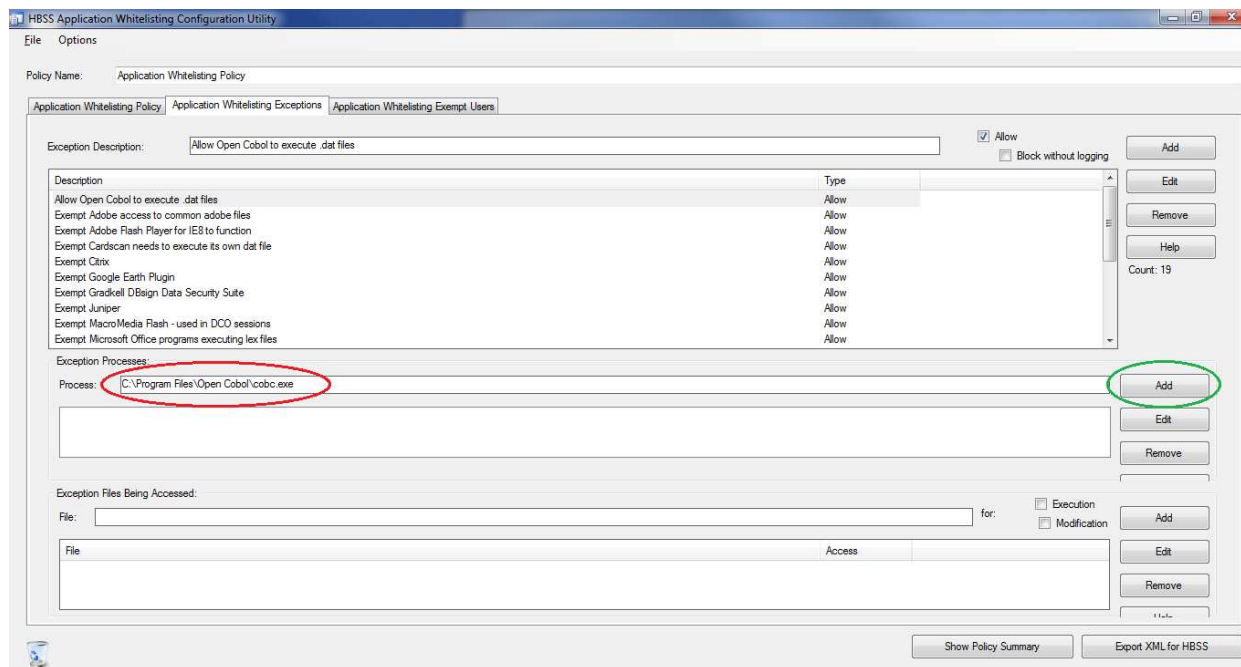
Click on the **Application Whitelisting Exceptions** tab



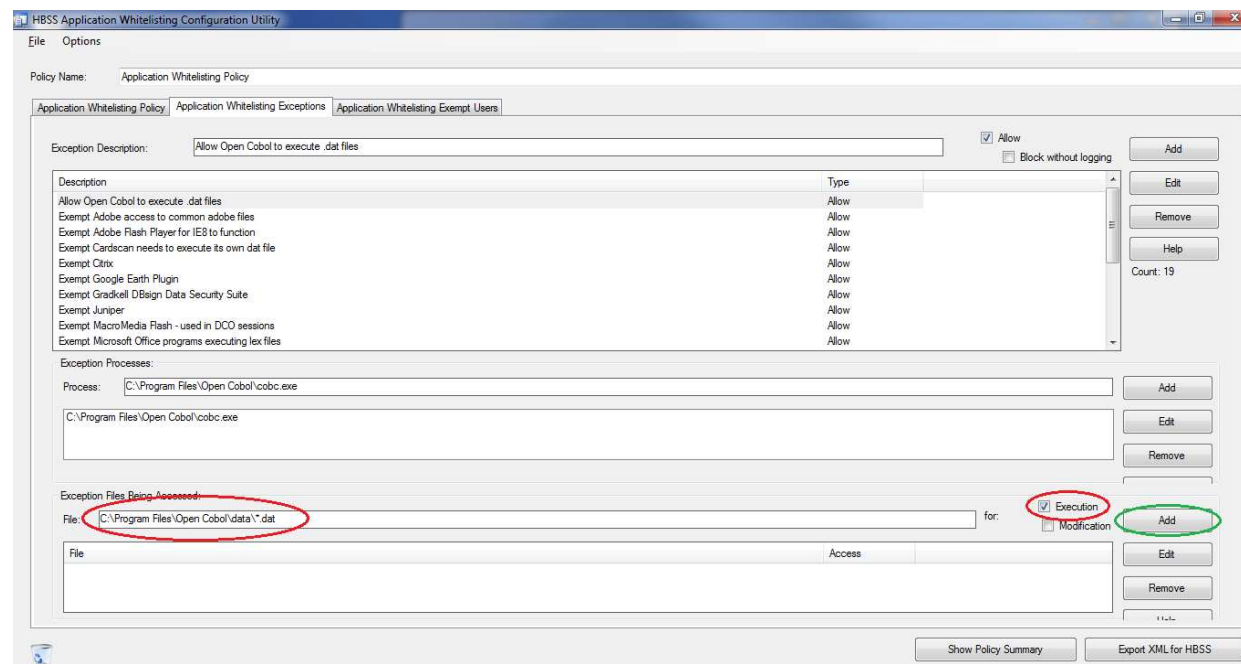
Type in a name for the exception in the **Exception Description** box, click on the **Allow** box, then click **Add**. If there is an existing exception that is similar to the new exception you are adding, consider adding to the existing exception instead of creating a new exception.



Type in the path (including name) of the program that you want to create an exception for in **Exception Processes**, then click **Add**. This can be done multiple times if you are adding more than one program.



Type in the extension of the files that you want your program to be able to execute in the **Exception Files Being Accessed** box, check the **Execution** box, then press **Add**. This can be done for more than one extension type. Be sure to include a “*.” before the extension name. It is a good idea to narrow down what directories this extension can be executed from. If you know what directories the file will be executed from then be sure to use the directory paths instead of allowing execution globally. (Example: If .dat files are always executed from C:\Program Files\Open Cobol\data\ then use C:\Program Files\Open Cobol\data*.dat instead of just *.dat)

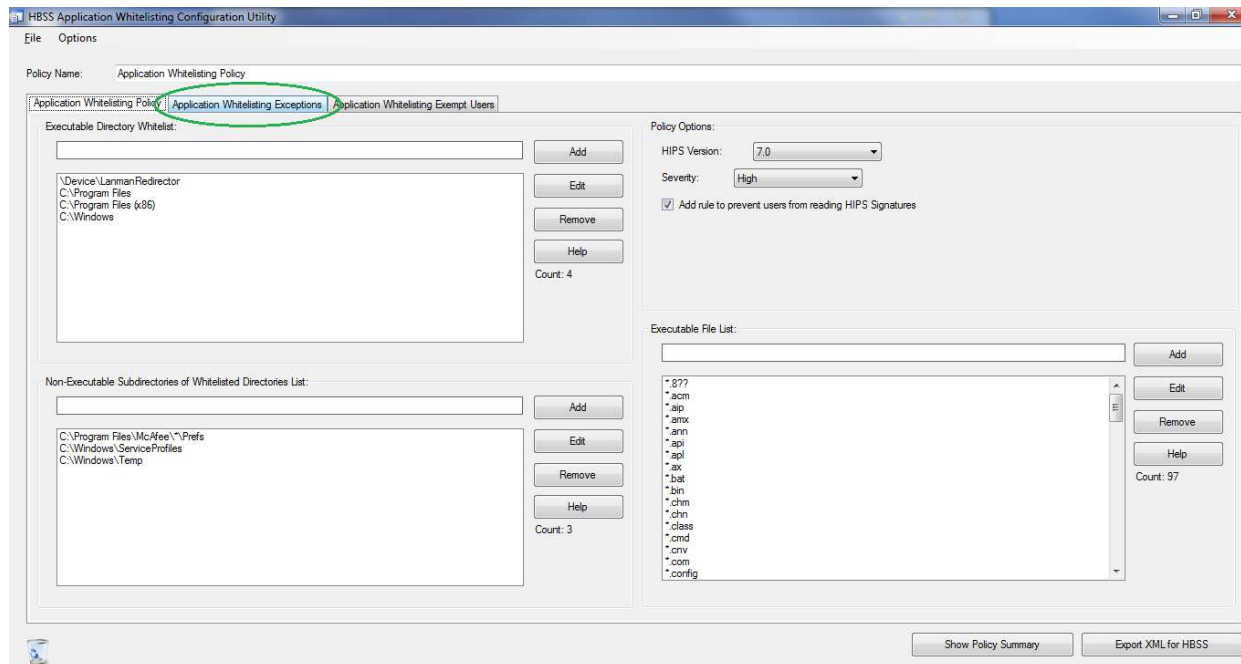


Be sure to save any changes that you make to your policy.

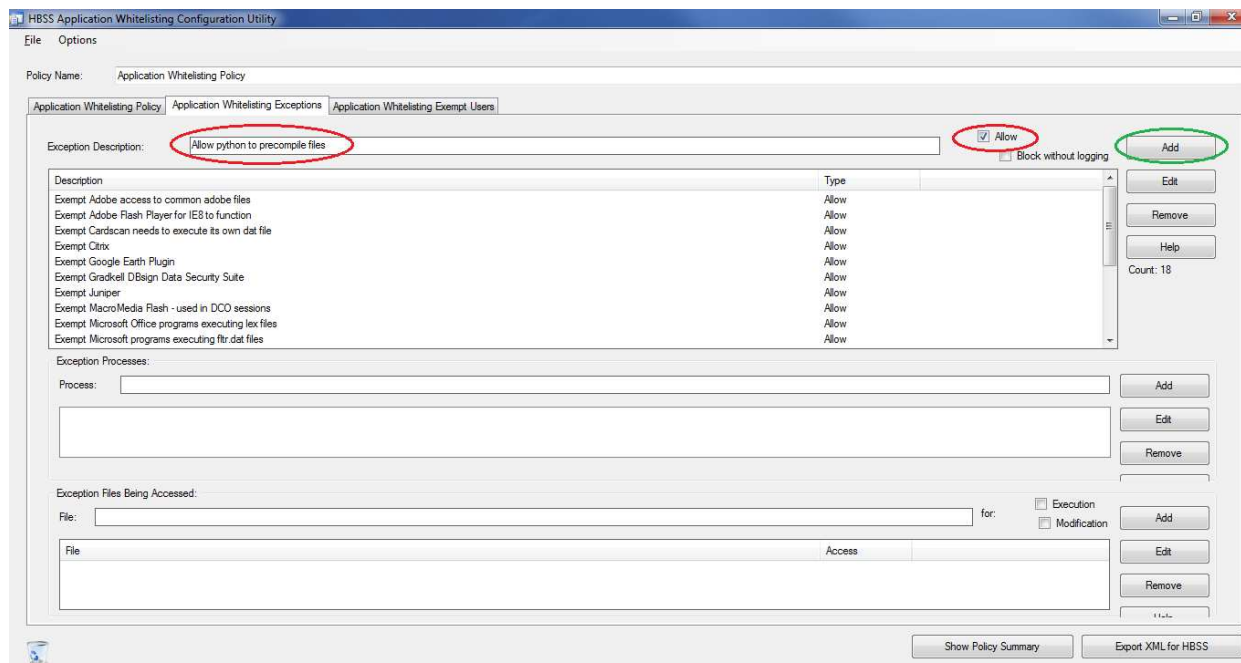
Add a carefully constrained modification rule

Open the HBSS application whitelisting configuration utility.

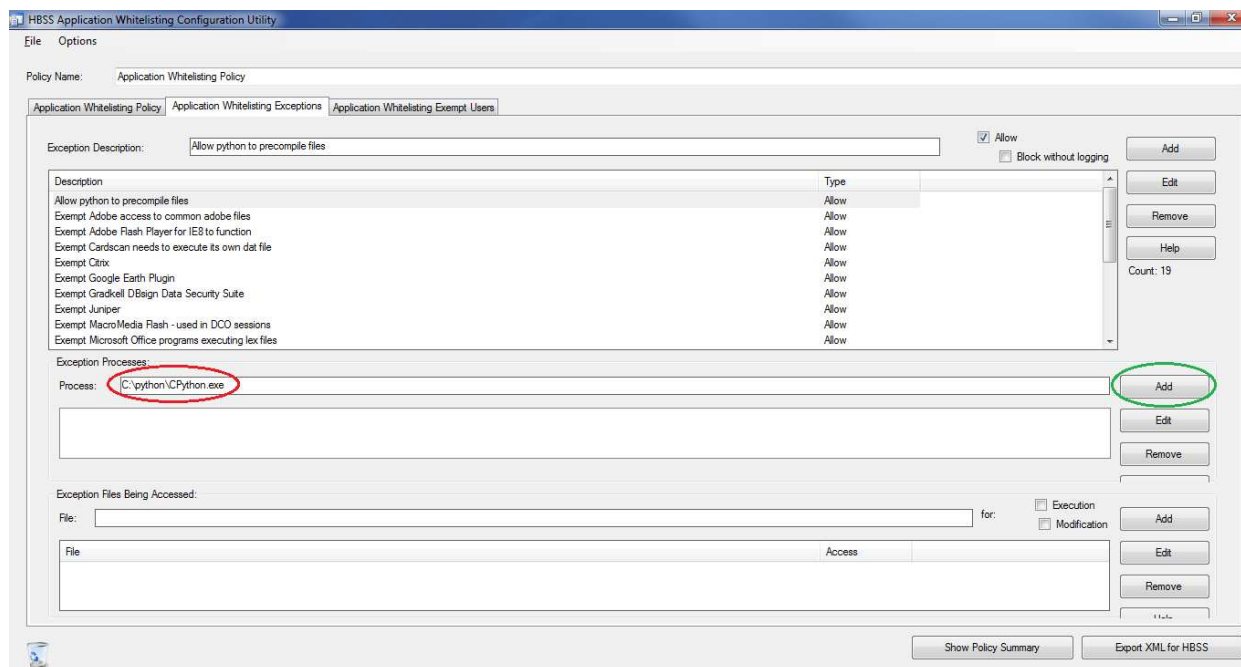
Click on the **Application Whitelisting Exceptions** tab.



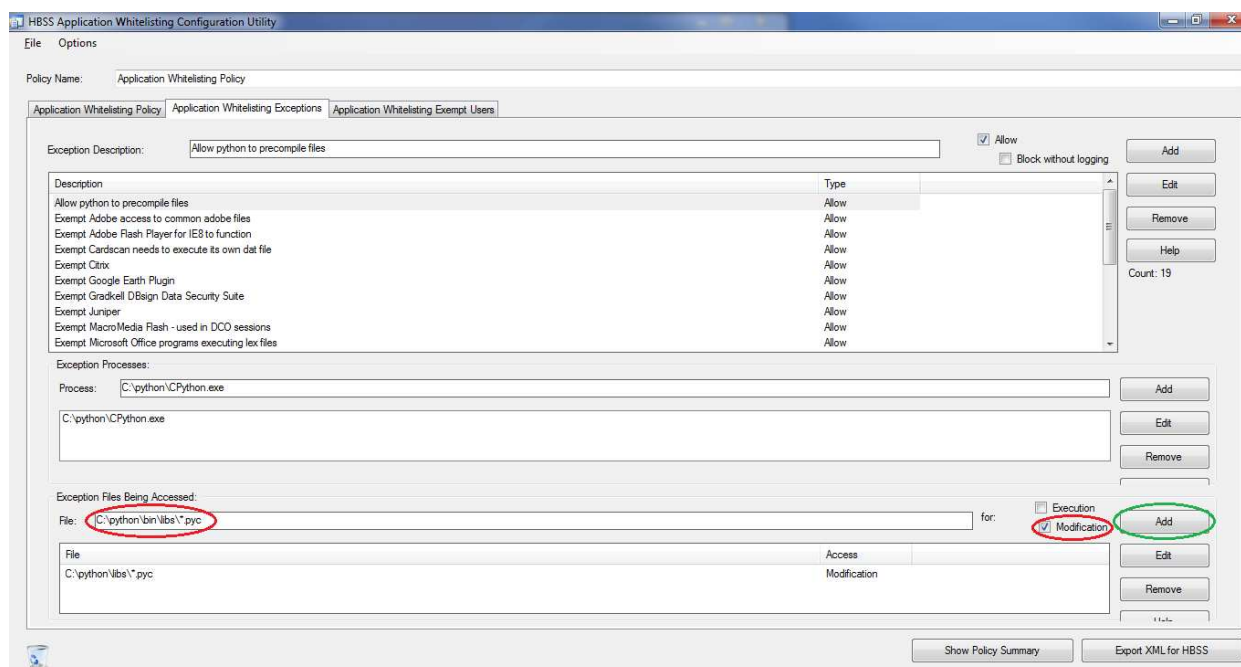
Type in a name for the exception in the **Exception Description** box, click **Allow**, then click **Add**.



Type in the name of the program that will be allowed to modify certain executable files into the **Exception Processes** box then click **Add**. If there is an existing exception that is similar to the new exception you are adding, consider adding to the existing exception instead of creating a new exception.



In the **Exception Files Being Accessed** box, type in the files that the program will be allowed to modify. Click the **Modification** box, then click **Add**. It is very important that any rules you create are as specific as possible while at the same time not requiring too many exceptions. Rules that are too general could cause the application whitelisting implementation to become ineffective.



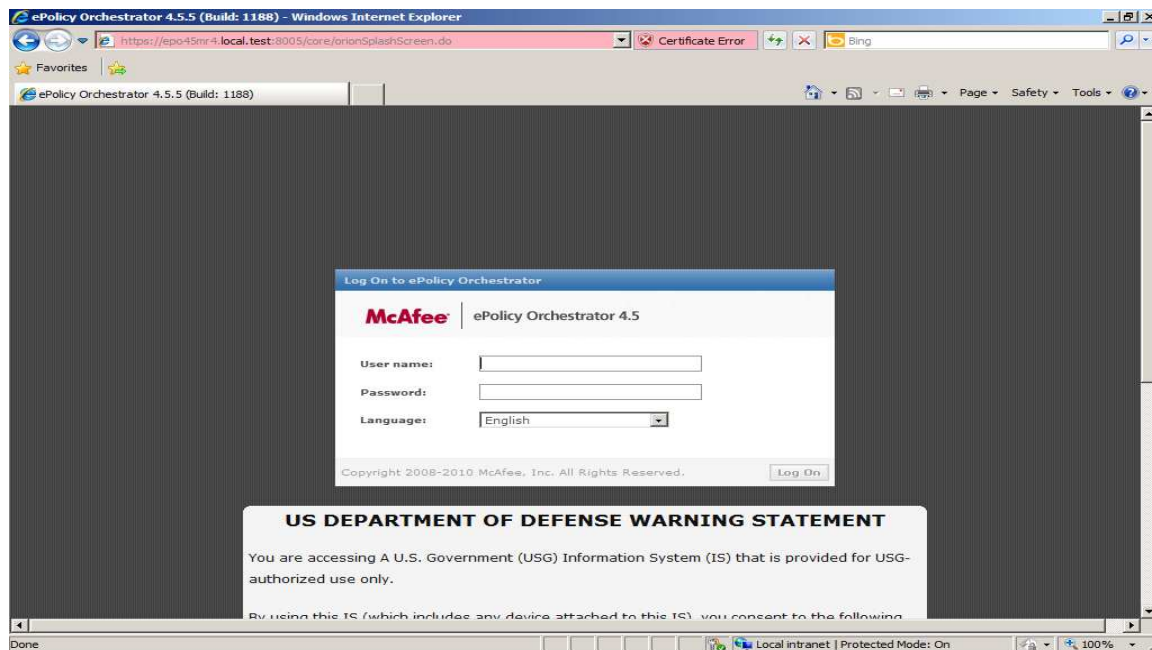
Be sure to save any changes that you make to your policy.

Enforcement

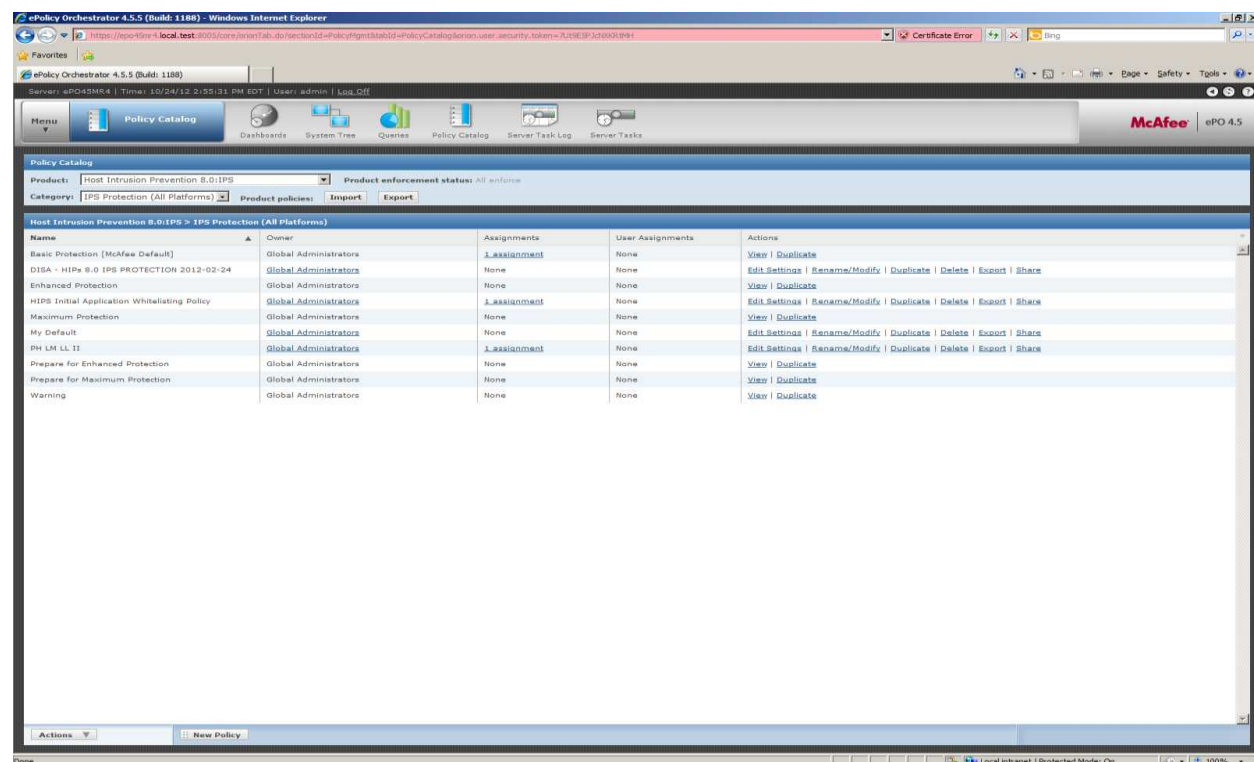
After you have tailored the application whitelisting policy for your network based on the auditing that you did, you will enforce the new policy. Follow the steps below to enforce your new policy.

Applying HIPS policies to a group

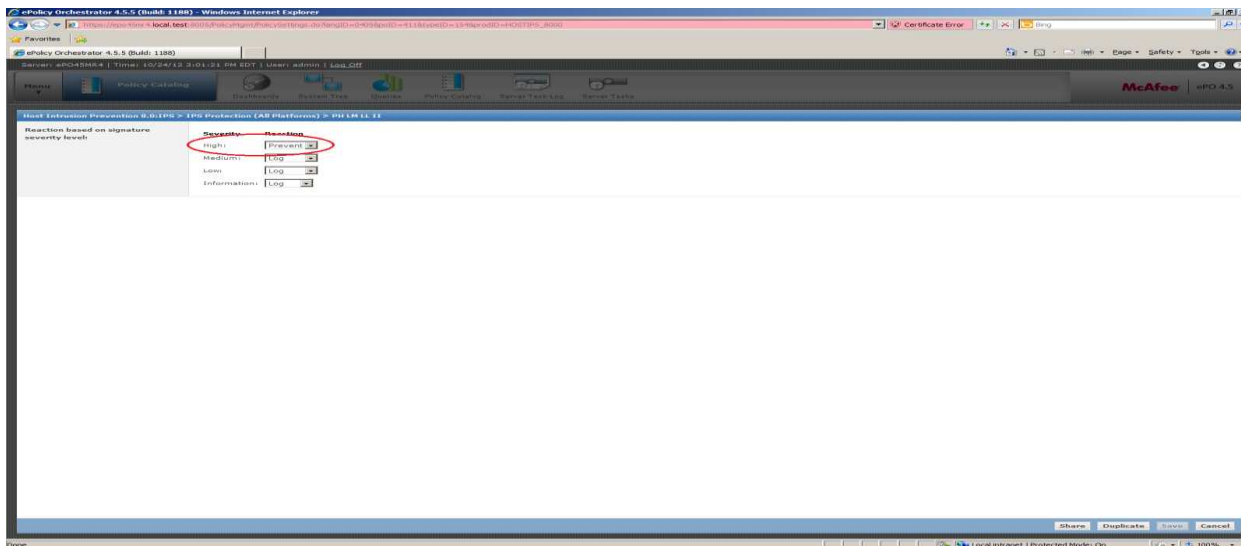
Log into the ePO server



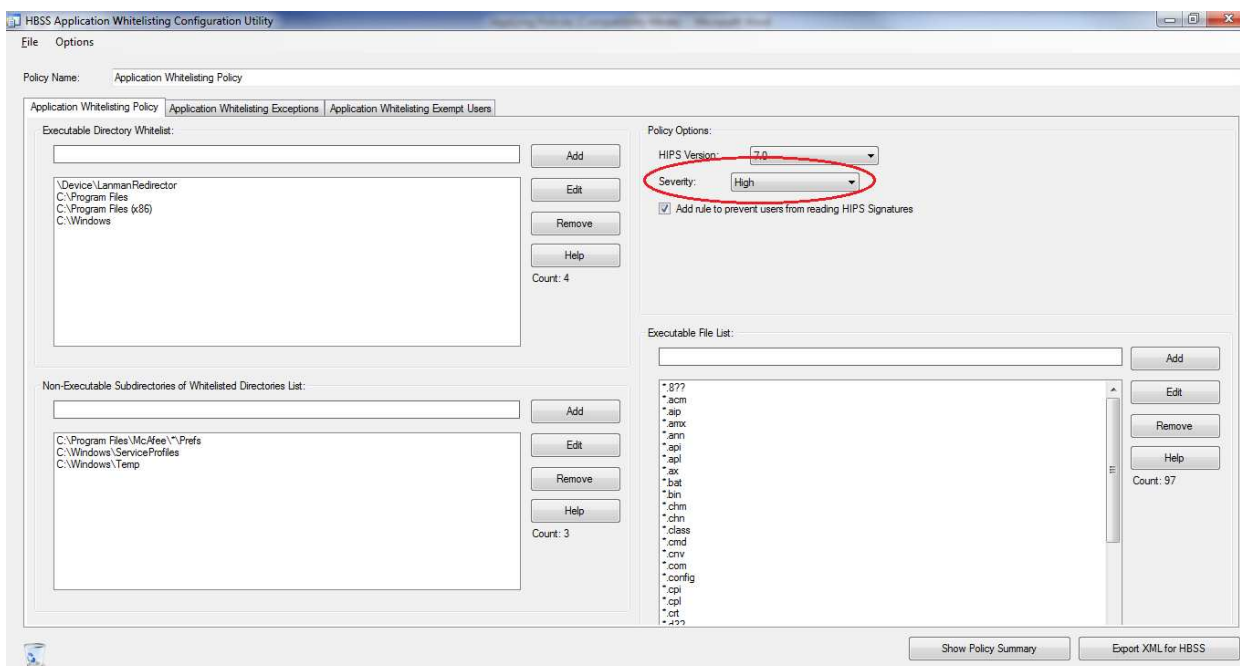
Click on the Policy Catalog tab



Select Host Intrusion Prevention 7 IPS or Host Intrusion Prevention 8 IPS from the product tab depending on what version you are running. Next, regardless of your version, you will select the “IPS Protection (All Platforms)” in the “Category” dropdown menu (which is located below the “Product” dropdown menu). Under the assignments column, find the assignment that is assigned to “My Organization”. Once you have located the policy that is assigned to “My Organization” click on edit settings under the actions tab. Find the severity category that has “prevent” set as the reaction. Take note of what the severity is.



Go to the HBSS application whitelisting configuration utility and under policy options set the severity level to the same level that you took note of in the last step.

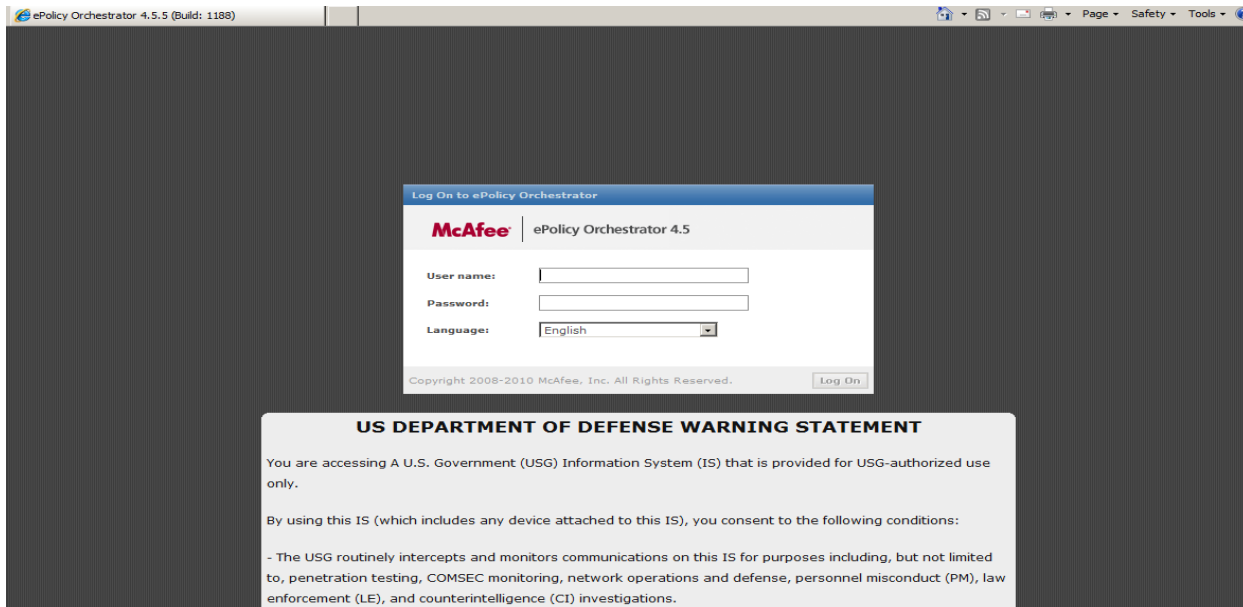


Export the policy to the local desktop by clicking on “File” then “Export XML for HBSS”.

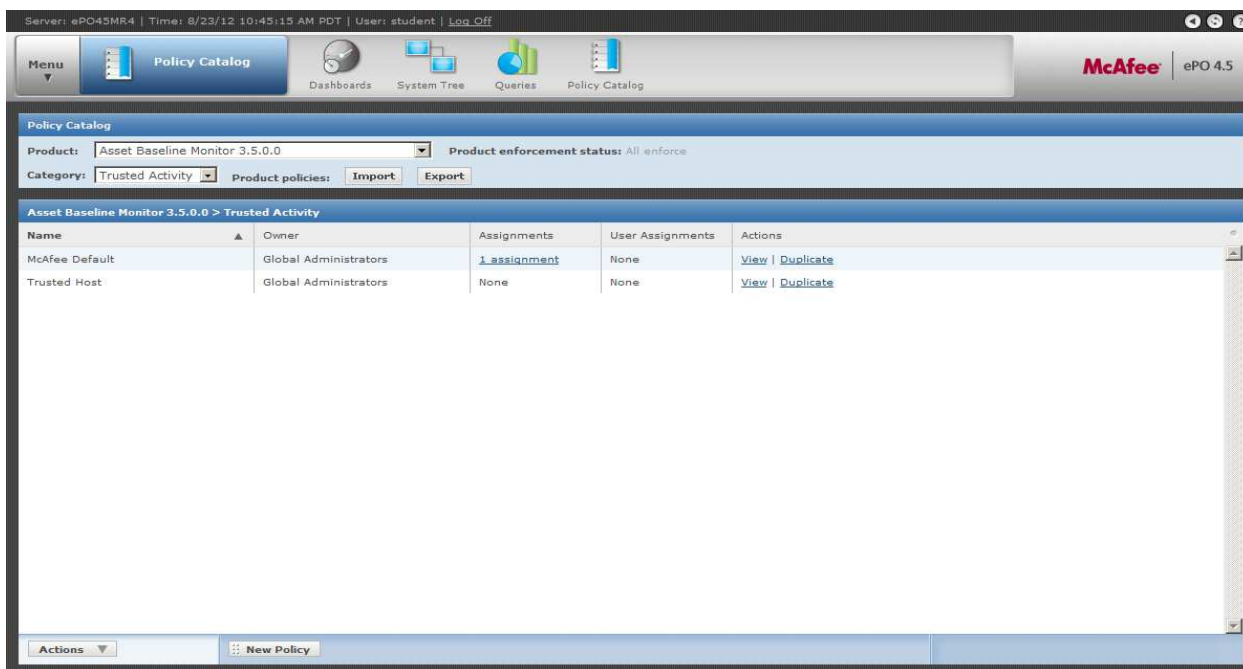
Be sure to use a unique name for your policy. If you do not then you could overwrite another policy.

Next you will import your custom policy into the ePO server:

Log into the ePO server



Navigate to the “Policy Catalog” tab.



Select the Correct Version of HIPS in the “Product” drop down menu (in the example below, we are running HIPS 8). The Name you will select will be similar to “Host Intrusion Prevention 7.0.5:IPS” or “Host Intrusion Prevention 8.0:IPS” depending on which version you are running. It will look like one of the following screens depending on your version:

This is if you are running HIPS 8:

Server: ePO45MR4 | Time: 8/23/12 10:48:03 AM PDT | User: student | [Log Off](#)

Menu Policy Catalog Dashboards System Tree Queries Policy Catalog **McAfee** ePO 4.5

Policy Catalog

Product: Host Intrusion Prevention 8.0:IPS Product enforcement status: All enforce

Category: IPS Protection (All Platforms) Product policies: Import Export

Host Intrusion Prevention 8.0:IPS > IPS Protection (All Platforms)

Name	Owner	Assignments	User Assignments	Actions
Basic Protection [McAfee Default]	Global Administrators	1 assignment	None	View Duplicate
DISA - HIPS 8.0 IPS PROTECTION 201	Global Administrators	None	None	Edit Settings Rename/Modify Duplicate Delete Export Share
Enhanced Protection	Global Administrators	None	None	View Duplicate
Maximum Protection	Global Administrators	None	None	View Duplicate
My Default	Global Administrators	None	None	Edit Settings Rename/Modify Duplicate Delete Export Share
PH LM LL II	Global Administrators	1 assignment	None	Edit Settings Rename/Modify Duplicate Delete Export Share
Prepare for Enhanced Protection	Global Administrators	None	None	View Duplicate
Prepare for Maximum Protection	Global Administrators	None	None	View Duplicate
Warning	Global Administrators	None	None	View Duplicate

Actions New Policy

This is if you are running HIPS 7:

Server: ePO45MR4 | Time: 8/23/12 10:50:04 AM PDT | User: student | [Log Off](#)

Menu Policy Catalog Dashboards System Tree Queries Policy Catalog **McAfee** ePO 4.5

Policy Catalog

Product: Host Intrusion Prevention 7.0.5:IPS Product enforcement status: All enforce

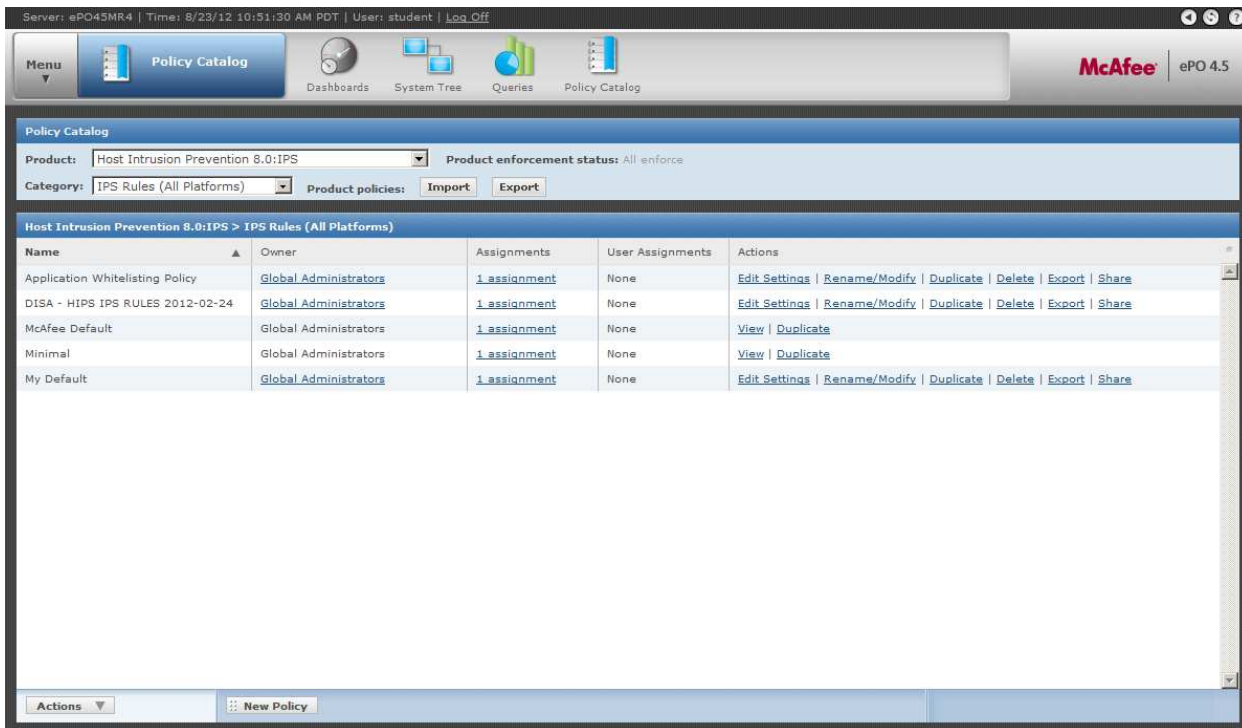
Category: IPS Options (All Platforms) Product policies: Import Export

Host Intrusion Prevention 7.0.5:IPS > IPS Options (All Platforms)

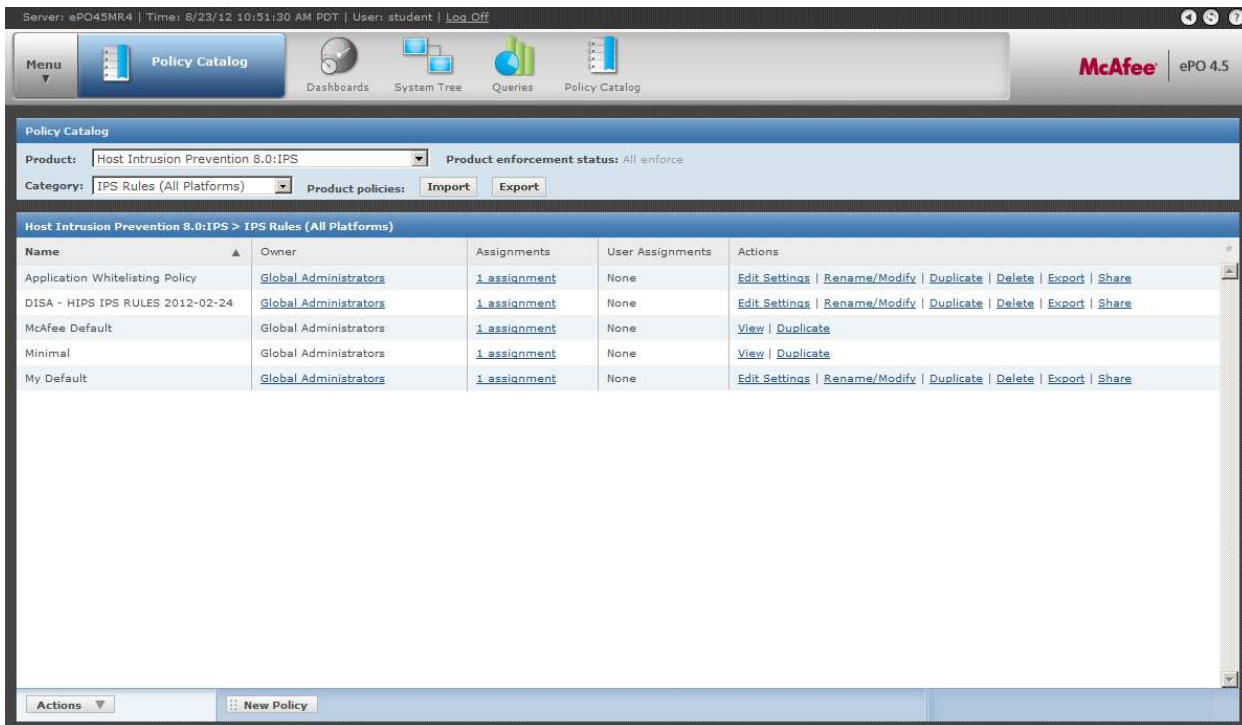
Name	Owner	Assignments	User Assignments	Actions
Adaptive	Global Administrators	None	None	View Duplicate
My Default	Global Administrators	1 assignment	None	Edit Settings Rename/Modify Duplicate Delete Export Share
Off	Global Administrators	None	None	View Duplicate
On [McAfee Default]	Global Administrators	1 assignment	None	View Duplicate

Actions New Policy

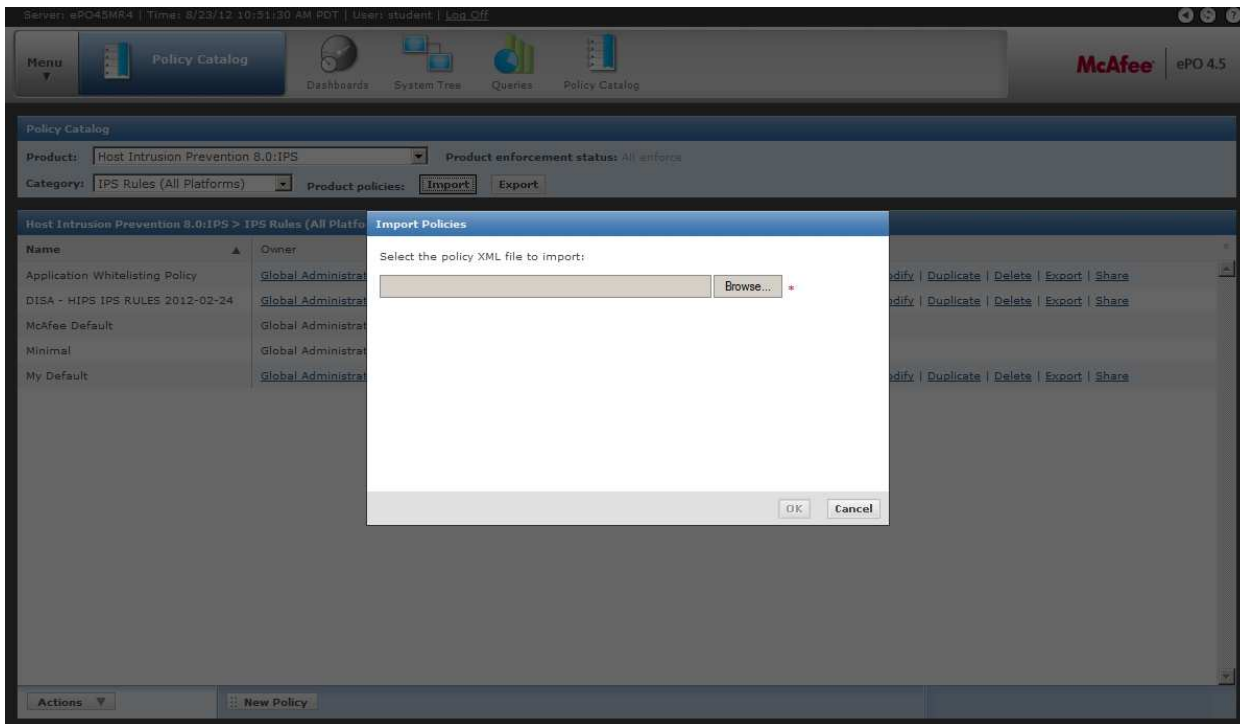
Next, regardless of your version, you will select the “IPS Rules (All Platforms)” in the “Category” dropdown menu (which is located below the “Product” dropdown menu)



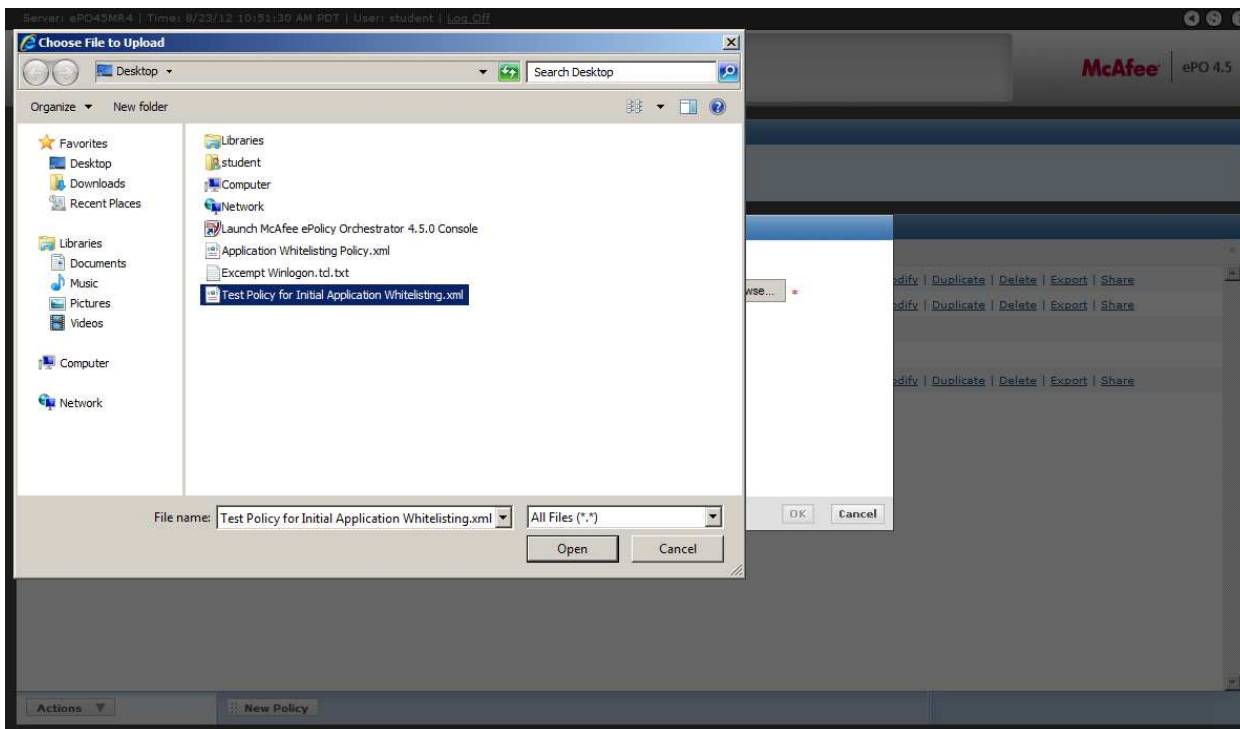
You will see a screen with a list of the currently available HIPS policies on your ePO server. Next Click the “Import” Button, to the right of “Product policies:”



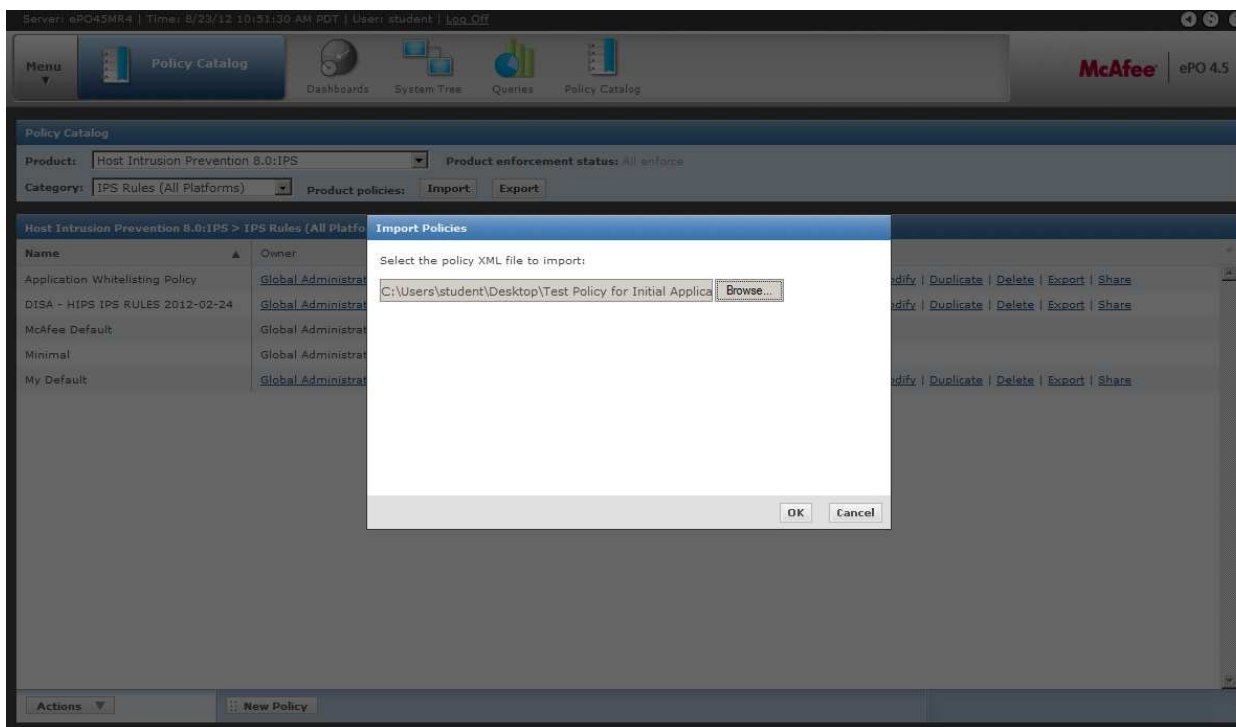
A new window will display as shown: Click “Browse” to navigate and select the policy file you exported from the application whitelisting application.



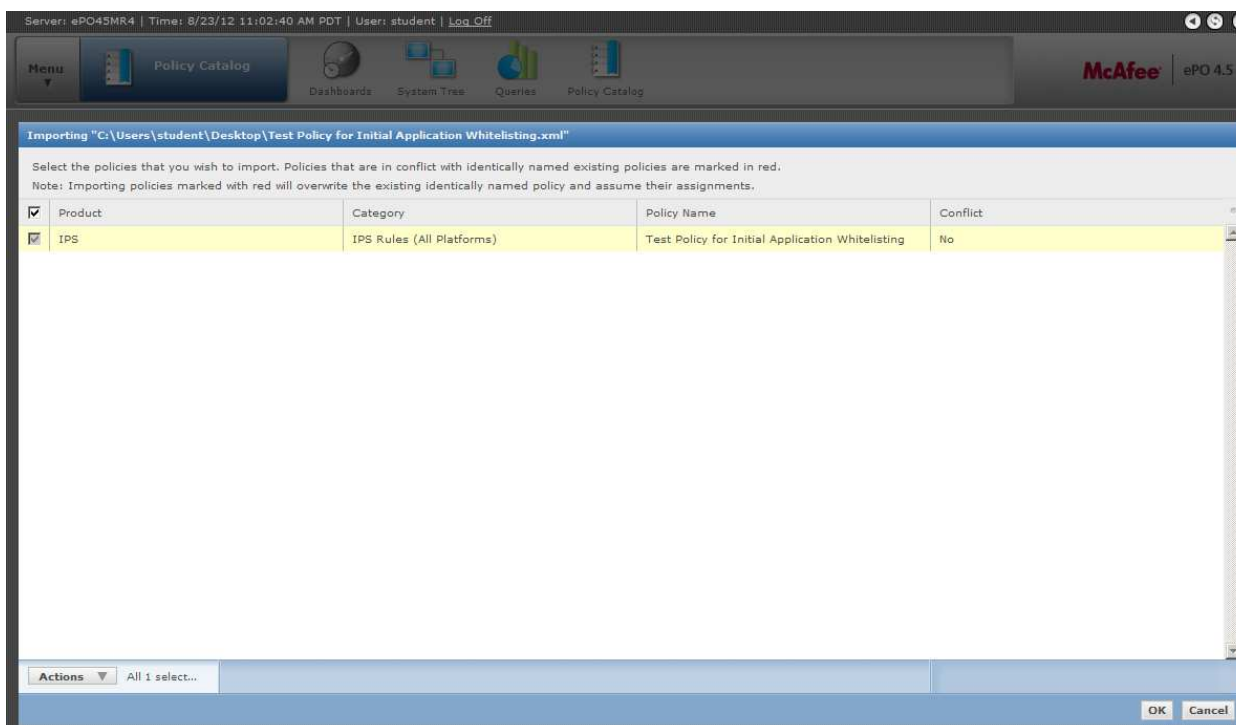
Here is a screenshot of the browse window that pops up when you click the “Browse” button.



Once you click, “Open” the following window will be displayed:

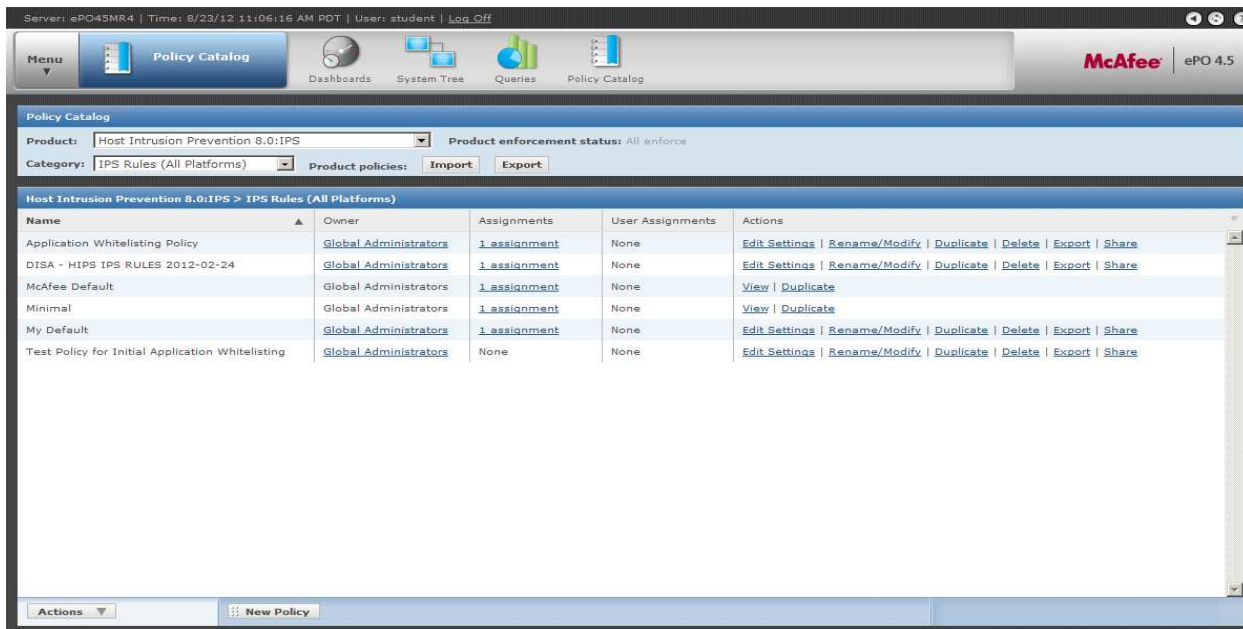


Click “OK” to confirm the policy import. The window below will be displayed:



Make sure the conflict column states "No". If the conflict column states "Yes", you will need to go back to the Application Whitelisting tool and rename the policy and repeat the steps above to import the policy with no name conflicts.

Click “OK” to confirm the policy import again. You will be brought back to the main HIPS policy screen. Make sure your policy name is now in the list. If it is, you have successfully imported the new policy.

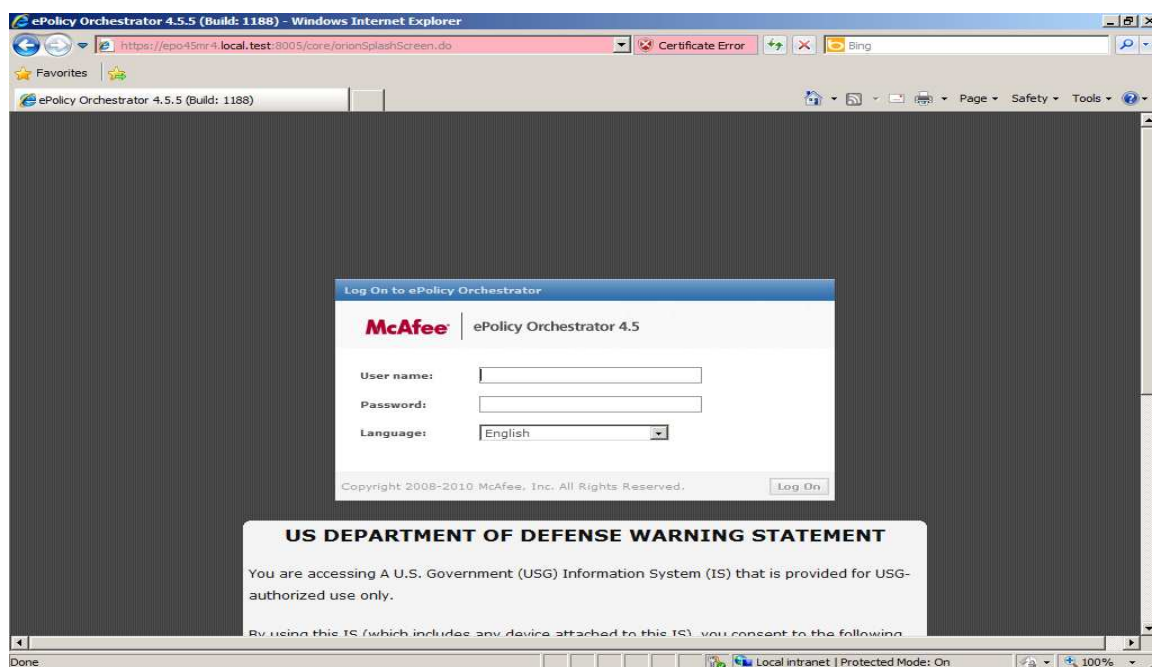


If you do not see your policy in the list, make sure you have navigated to the correct “Product:” and “Category:” sections. Make sure you have rights to import policies, and make sure you are not using a duplicate name which causes a policy conflict.

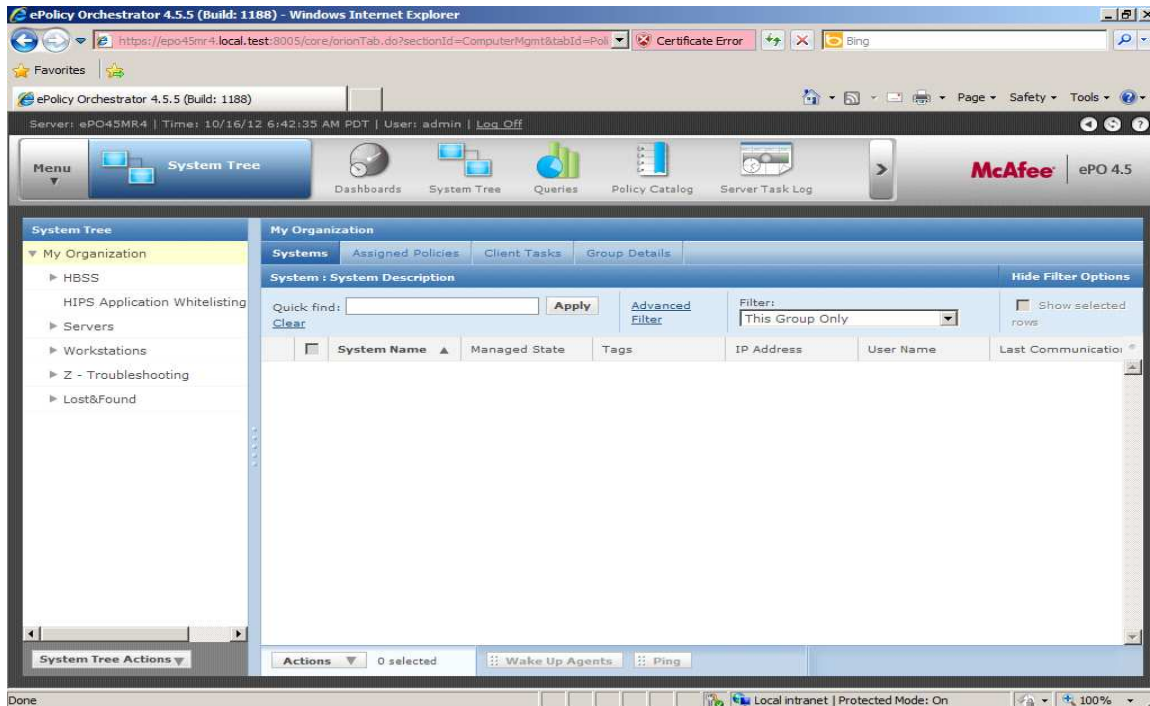
You have now successfully imported your enforceable application whitelisting policy!

Next you will apply your custom policy.

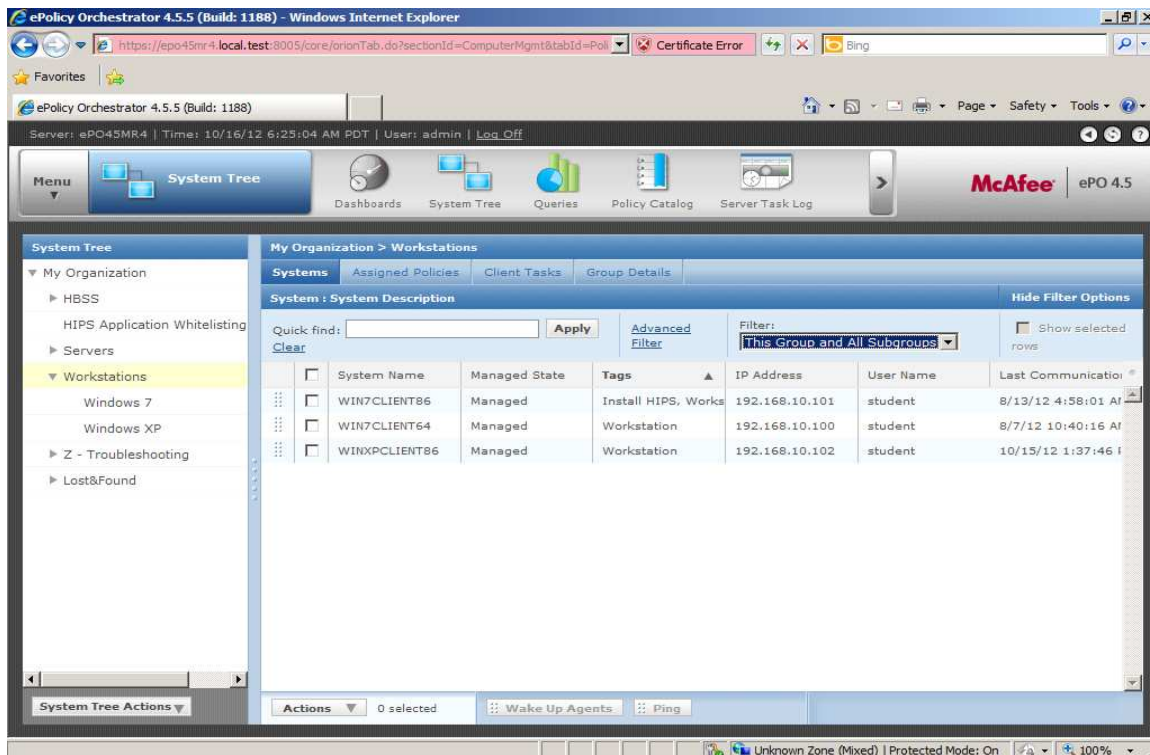
Log into the ePO server



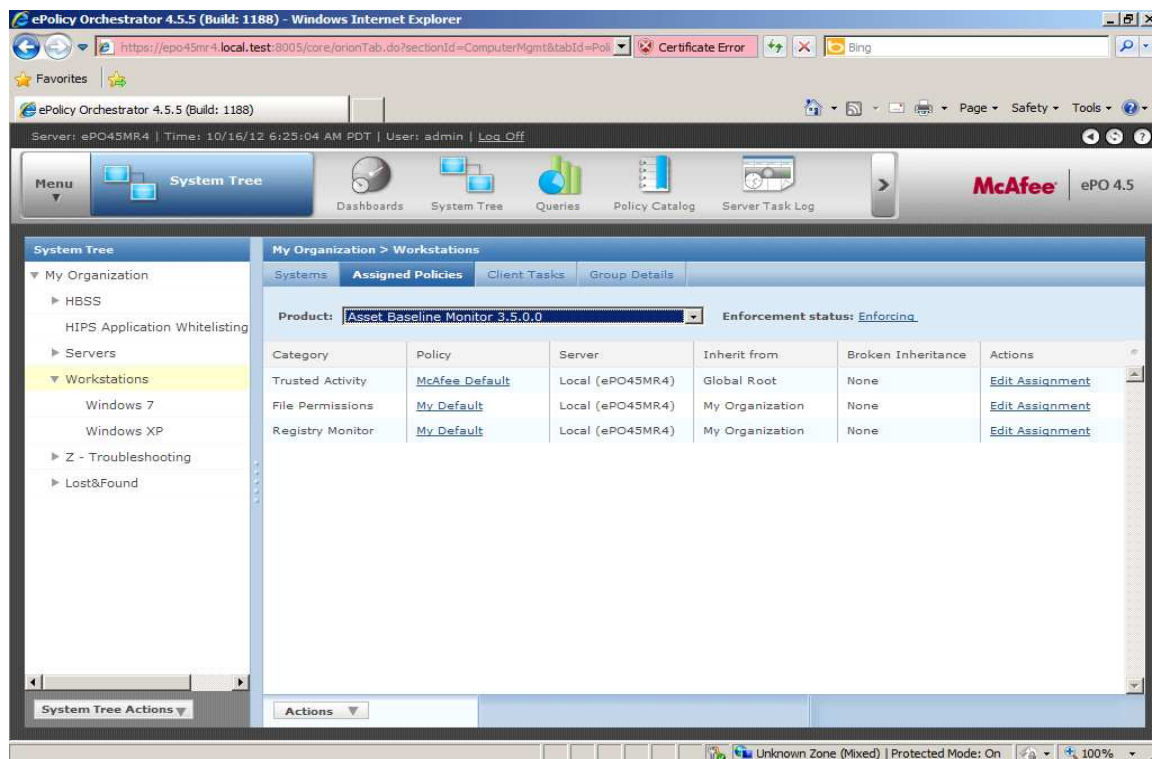
Navigate to the “System Tree” Tab.



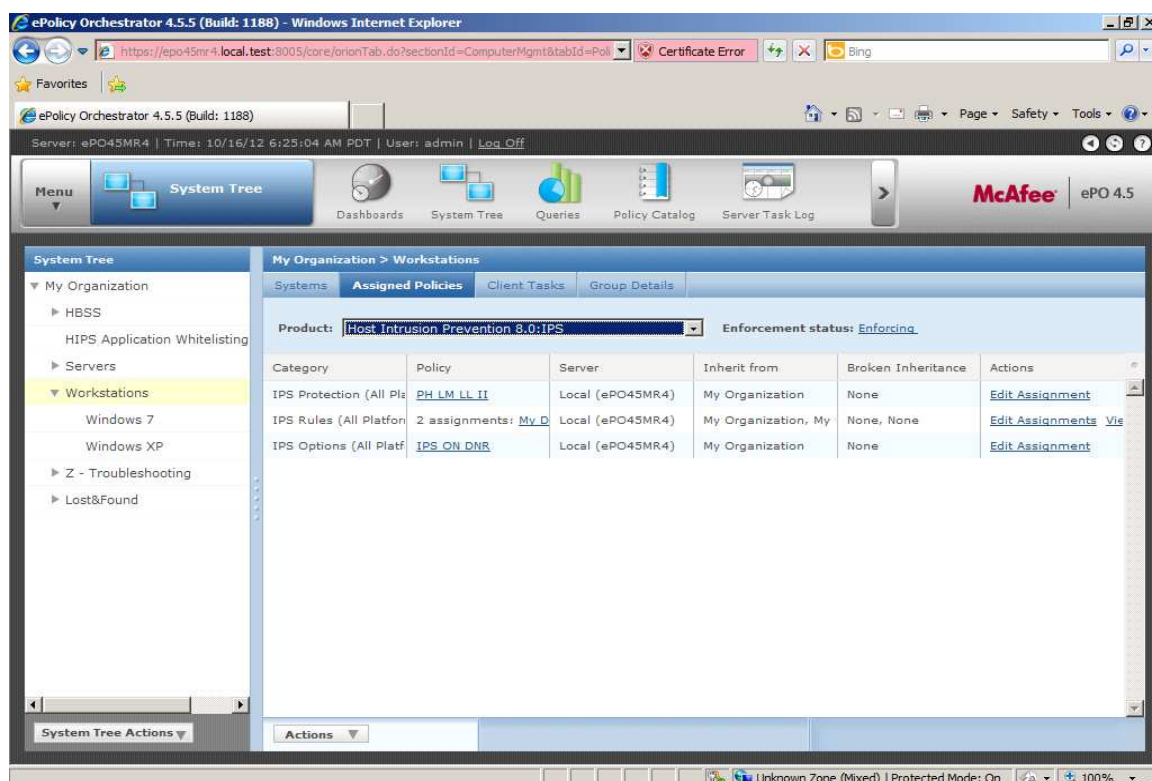
Select the container that you want to apply the new policy to. In our case, this container is called, “Workstations”. In general when enforcing the policy, first start small with your test group then gradually apply the policy to larger and larger containers up the ePO system tree hierarchy. Selecting the container will display the machines in that container. Make sure all machines that will be assigned the new policy are in the container. If all machines that will be assigned the new policy do not show up, change the filter setting to “This Group and All Subgroups” so that all subgroups will be displayed.



With your container selected, click on the “Assigned Policies” Tab. This will bring up the policies assigned to your selected. You should see the window below.

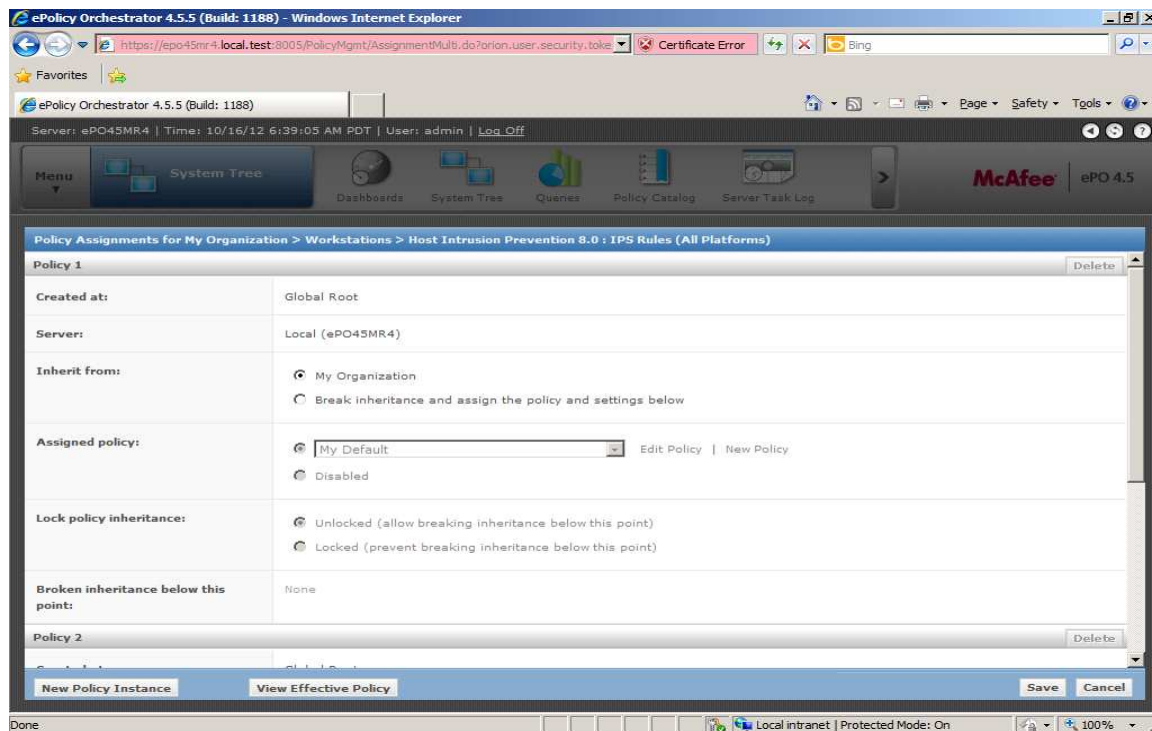


In the “Product” dropdown menu, select the version of HIPS you are running (7 or 8). The screen will look as follows. Your display may look slightly different if you are navigating to the HIPS 7 module in the “Product” dropdown menu.

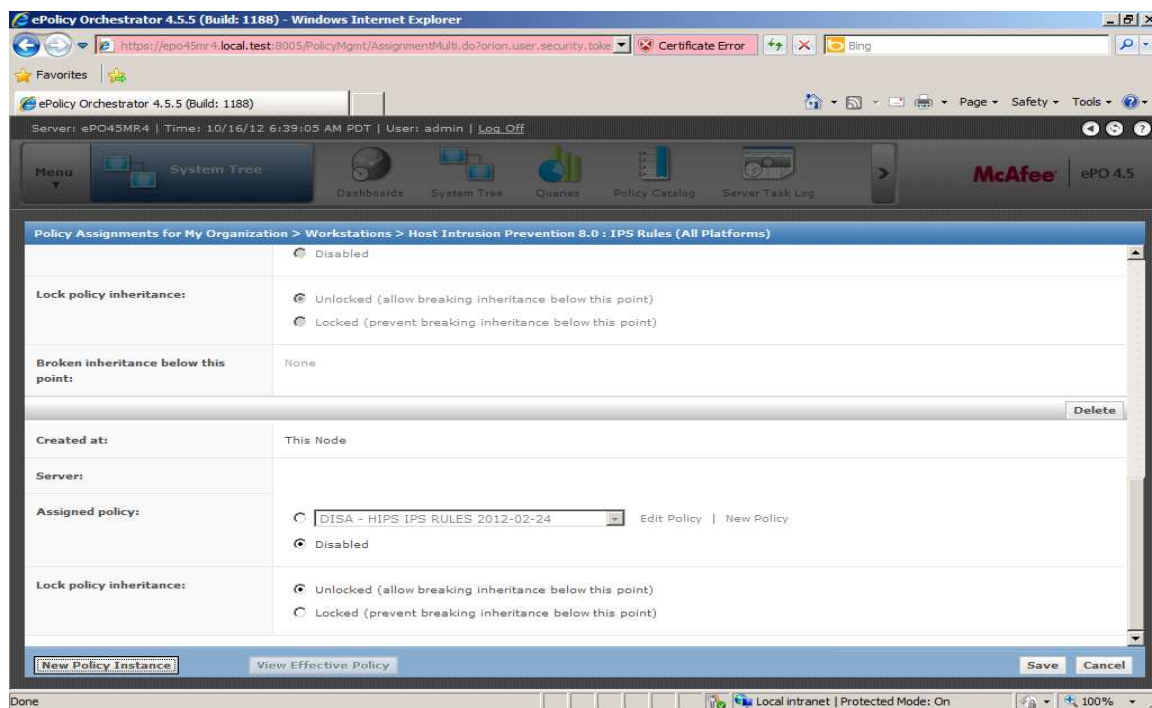


In the “Category” column, find the entry that says, “IPS Rules (All Platforms)”, click “Edit Assignments” to edit the IPS Rules policies that are assigned to your test containers.

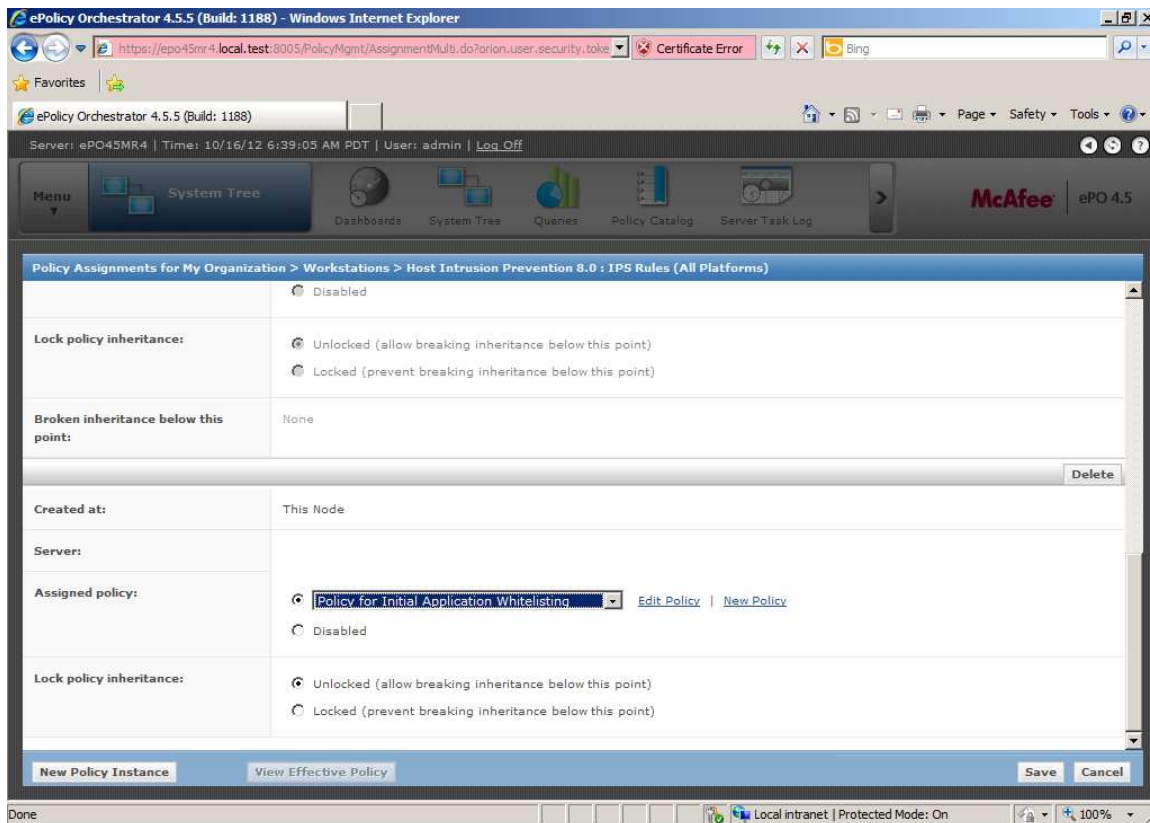
The following screen will be displayed once you click the “Edit Assignments”:



Click “New Policy Instance” to create a new section to make a new policy assignment. The new section will be appended to the end of the current assignments. (Use the scroll bar to scroll down if needed).



Now assign the HIPS Rules Policy you created by clicking the radio button and selecting your policy name. Make sure the radio button “Unlocked (allow breaking inheritance below this point)” is also selected.



Click Save to apply your policy to your selected group on the ePO server. Congratulations, you have successfully applied your enforced application whitelisting policy to be enforced on your selected container.

Monitoring

Reviewing events

You should review events on a regular basis. Reviewing events will help you find malicious activity on your network. If there are too many events to look through, consider adding rules to block without logging common events, this will help you locate more important events. [How to block without logging](#), page 55

How to pick out more important events

It can be difficult to pick out important events from large log files. Most things in log files can probably be ignored. There are several things that you can look for to try to find important things in log files. The first thing to look for is a lot of execution attempts or a spike of execution attempts from a single machine or a small group of machines especially if those execution attempts come from obscure directories. Another important thing to look for is a lot of attempted executions from temp directories. Normally programs do not need to execute things from the temp directory so be suspicious when there are a lot of attempted executions from a temp directory. Another thing to look for is programs trying to execute other programs when they would not normally do that. An example of this could be adobe reader trying to execute cmd, normally adobe reader does not execute programs other than other adobe programs. Be sure to look at things that are executed from a temporary internet folder. A lot of attacks against web browsers will result in an

execution from a temporary internet folder. Also if users try to download and run something from the internet (which should not be allowed) the attempted execution will probably be from a temporary internet file depending on which browser is being used. This is not an all-inclusive list of things that you should look for when reviewing log files but should serve as a guideline of things to look for. Remember, if something looks suspicious then you should investigate it further. The numerical grouping in the auditing queries discussed earlier can help you identify anomalous events that are more suspicious.

Remediation and Tailoring when something breaks

When something breaks review the logs to see what is causing the program to fail then use the decision trees that are provided in this document to decide if the policy should be changed or an exception added to fix the problem.